



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 1

Thursday 1 October 1998

Contents

- [Computer collapse wipes out British Social Security records](#)
[PGN](#)
- [Calling All Traffic Lights in Dublin!](#)
[Fiachra O Marcaigh](#)
- [Y2K "fix" causes Dublin traffic jams](#)
[Mich Kabay](#)
- [Natural gas plant explosion in Victoria, Australia](#)
[Martin Gleeson](#)
- [Malaise in Malaysia hits satellite uplink](#)
[Mich Kabay](#)
- [Bank of Montreal card functions paralyzed by bug](#)
[Mark Brader](#)
- [Bad power strip knocks out Net service](#)
[Andrew Brandt](#)
- ["Cyberdeath" raises privacy issue](#)
[Scott Peterson](#)
- [How to bypass those pesky firewalls](#)
[Mark Jackson](#)
- [Hacking, Irish-Style](#)
[Fiachra O Marcaigh](#)

- [Re: X-rated net suit](#)
[Rishiyur S. Nikhil](#)
 - [Re: Sexy risks of searching for MP3](#)
[John Mee](#)
[Don Byrd](#)
 - [Y2K risk in Netscape cookies](#)
[J Seymour](#)
 - [Re: "Windows NT Security"](#)
[Russ Cooper](#)
[Joe Thompson](#)
 - [Enquiry re: problems at universities](#)
[Pete Mellor](#)
 - [REVIEW: "Decrypted Secrets", F. L. Bauer](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Computer collapse wipes out British Social Security records

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

Thu, 1 Oct 98 17:12:24 PDT

A major outage of the British Department of Social Security (DSS) national insurance register computer system (NIRS) has created a turmoil. Payments are being made manually without the usual vetting of eligibility. DSS is apparently being very coy about the situation, fearing a flurry of false claims. This occurred during the cutover to the new system (being developed by Andersen Consulting under a 170-million-pound project, reportedly the biggest and most complex information technology project in Europe). DSS officials anticipate that NIRS could be down until at least the end of October, although Andersen folks think they are close to solving

the
problem. Stay tuned. [Source: An article by David Brindle,
Guardian
Weekly, 20 Sep 1998, p. 10, courtesy of David Stringer-Calver;
PGN
Abstracting]

✈ Calling All Traffic Lights in Dublin!

"Fiachra O Marcaigh" <fiachra@iol.ie>

Tue, 29 Sep 1998 13:57:32 GMT

Getting into, or out of, Dublin City Centre by car was much more
difficult
than usual yesterday (Sept 28th, 1998). The journey that should
have taken
me 25 minutes (long after normal rush-hour at 9.30) took over an
hour
instead. During rush hour, one motorist reported taking an hour
and a half
to cover a mile and a half. In my case the congestion was so
severe in the
inner city that I kept expecting to round a corner and find some
major
obstruction such as a collapsed building, or two stalled trucks
side by
side.

The answer was much simpler - an incomplete "upgrade" had
disconnected the
traffic lights at 140 junctions from the Dublin Corporation
control
centre. The lights are normally regulated to cater for traffic
conditions,
but without communications they were left to get on with the job
themselves. They ran through preprogrammed sequences without
allowing for
traffic conditions, or proper synchronisation between them.
Gridlock
resulted.

PS: Yesterday's jams were so bad that traffic today was much *lighter* than usual. Thousands of people must have taken to public transport.

Full story: <http://www.irish-times.com/irish-times/paper/1998/0929/fro2.html>

[Also noted by
Niall Smart <nialls@euristix.ie>,
Bernard Lyons <bernardl@indigo.ie>.

See the next item from Mich Kabay, which provides a Y2K link!
PGN]

⚡ Y2K "fix" causes Dublin traffic jams

Mich Kabay <mkabay@compuserve.com>
Tue, 29 Sep 1998 09:12:43 -0400

Chris Parkin of *The Press Association News* (UK) reported that the Dublin traffic snarl on 29 Sep 1998 was due to poor quality assurance in a new version of the software controlling traffic signals led to fixed cycles with no allowance for longer cycles at peak traffic times. Ironically, the software was installed to prevent Y2K problems. [PGN edited]

This case illustrates

- * the general danger of introducing new bugs in any "fix" if QA procedures are inadequate;
- * the specific danger of pushing Y2K fixes into production without proper QA;
- * the vulnerability of electronically-controlled infrastructure to interference.

M. E. Kabay, PhD, CISSP / Director of Education
ICSA, Inc. <<http://www.icsainc.net>>

✶ Natural gas plant explosion in Victoria, Australia

Martin Gleeson <gleeson@unimelb.edu.au>
Mon, 28 Sep 1998 09:30:59 +1000

Shortly before 1pm on 25 Sep 1998, a series of explosions ripped through the Number 1 Plant at the Esso gas processing installation at Longford in eastern Victoria. Two workers were killed and seven injured. Effectively all residents of the state (~5 million) have been required to turn off their gas supply and it is not known when services will be restored. It could be days, weeks or even months.

RISKS? This looks like an all-your-eggs-in-one-basket problem. There are four plants at the Longford facility, but an incident like this means that they must all be shut down until the cause of the explosion is established. A new gas pipeline from a neighbouring state was finished six weeks ago, but it can only bring enough gas in for hospitals and nursing homes and to keep the gas pipeline network itself from going completely belly-up (it is absolutely vital that gas stays in the pipes and no air or water gets in). It is expected that industry will be losing upwards of \$100 million per day and thousands of workers will be stood down.

Further information can be seen at <<http://www.theage.com.au/special/gas/>>.

Looks like cold showers for a while. :-)

Martin Gleeson, Webmaster, The University of Melbourne,
Australia.

<URL:<http://www.unimelb.edu.au/%7Egleeson/>>

[Also noted by

"Martin, Mike" <mmartin@sbns.com.au>, who noted the effects
on industry and on the spectators of the Australian
Football

League grand final in Melbourne (perhaps linked to
Victoria losing

to South Australia because they did not want cold
showers?),

Toby Stevens <Toby.Stevens@pa-consulting.com>, who noted that
the crematoriums were shut down, and

"Peter J. Cherny" <peterc@arquebus.com.au>.

PGN]

✶ Malaise in Malaysia hits satellite uplink

Mich Kabay <mkabay@compuserve.com>

Mon, 28 Sep 1998 17:15:38 -0400

As most readers will know, there is political unrest in Malaysia
because

the government has accused the former finance minister Anwar
Ibrahim

(who was also the deputy prime minister) with various unsavory
crimes

(which he and his supporters characterize as a smear campaign).

The following detail at the end of an article entitled,

"Matathir cracks

down on protests" by Nick Hopkins in this week's (1998.09.27)

_Guardian

Weekly_ (p. 4) caught my eye:

"Diplomatic relations were further strained when broadcasters, including the BBC, discovered that their reports were being censored by the Malaysian authorities. Footage of the clashes between police and protesters demanding the resignation of Dr Matathir was blacked out by hackers, who intercepted transmissions bound for a satellite link."

Jamming itself is hardly new, but if -- and I stress *_if_* -- this report is correct, it represents a rare case of known information warfare through an attack on communications satellites.

M. E. Kabay, PhD, CISSP / Director of Education
ICSA, Inc. <<http://www.icsainc.net>>

✦ Bank of Montreal card functions paralyzed by bug

Mark Brader <msb@sq.com>
Wed, 30 Sep 98 05:30:57 EDT

Yesterday morning at 5:30 am, a new software version was loaded on the computers that control all electronic card transactions at the Bank of Montreal. It was intended to upgrade the system to better handle the upcoming Christmas season. Instead the result was MasterCard credit authorizations denied, debit cards denied, and ATMs shut down.

According to today's **Toronto Star**, "bank technicians ... immediately set up 'war-rooms' -- rethinking pages and pages of computer code, desperately trying to find a quick solution." The article is silent on the

possibility
of quickly reverting to the previous version. Anyway, at 1:30
pm the system
"went down hard" and it wasn't until 4:30 that things were
working again.

The Bank of Montreal is the third-largest in Canada, and the
largest
MasterCard issuer. The Star article refers to 2,000,000
cardholders,
but isn't clear as to whether this is the total number of them
or the
number who actually use their cards in one day -- the figure
seems to me
too low for the one and too high for the other.

⚡ Bad power strip knocks out Net service

Andrew Brandt <anb@lanminds.com>

Wed, 16 Sep 1998 11:06:55 -0700

What follows is a message send by the sysadmin at my employer's
office. The
company for which I work has a huge number of employees who use
their Net
connection daily as part of their job duties.

The risk in this case is obvious. Major network hubs should have
proper
electrical power connections (with uninterruptable power
supplies) for
their servers and associated network hardware. Kludgy solutions
aren't
appropriate for large businesses. I can only assume somebody
blew it when
they didn't install the appropriate electrical hookups in their
server room,
and tried to cover their error by using power strips. Replacing
the power
strips is only a temporary fix, though I doubt more will be done

to correct
the problem.

How many other ISPs use \$5-20 power strips on their \$10,000+ hubs, routers, and servers, instead of wiring their offices correctly from the beginning? I suppose we'll just have to live with this idiocy for a while.

> Last night, two of the power strips feeding power to our network
> equipment in [city name deleted] failed. Power has been restored as
> well as our ability to surf the web and replicate using an ISP.

> The outage began sometime yesterday evening at around 6:45 PM and was
> temporarily fixed. This morning we noticed another outage which lasted
> for about 20 minutes. We're waiting to hear from our ISP to know more
> about the second outage. Our guess is that this morning's brief outage
> was necessary to transfer our equipment to new power strips. I'll
> confirm with our ISP this later today.

🔥 "Cyberdeath" raises privacy issue

Scott Peterson <scott4@ibm.net>
Fri, 25 Sep 1998 15:24:25 -0700

An article yesterday in my local paper crediting Cox News service relates the story of a woman who applied for a loan at her bank. However, the credit check indicated that Social Security said she was dead.

An investigation uncovered that a claims agent at the SSA's

Belle Glade FLA

office named Jorge Yong had had a fight with the woman in an internet chat room and was banned from it. In retaliation, he used a co-workers terminal to put a date of death on the woman's record.

Yong resigned and was ordered to pay \$700 to the victim and pay a \$100 fine after pleading guilty to one count of falsifying personal data

This story came out in testimony by acting inspector general James Huse before the Senate Governmental Affairs Committee as part of an ongoing investigation of whether private information is safe on government computers.

Scott Peterson <ScottP4@IBM.NET>

⚡ How to bypass those pesky firewalls

Mark Jackson <mjackson@wc.eso.mc.xerox.com>

Tue, 29 Sep 1998 11:30:43 PDT

The United Media website (very popular as it is the home of the "Dilbert Zone") is advertising "Comic Explorer - the NEW way to read comics." Turns out (<http://www.unitedmedia.com/explorer/index.html>)

that it's a free "Java" applet that facilitates browsing their comics archives - if you have a Pentium running Windows (hence the quotes around "Java").

But click on "System Requirements" and one finds the following advisory:

Firewalls:

Some companies have firewalls that make it difficult to run Java

applets with multiple classes. If this is the case, you can make

some adjustments to use the software with Internet Explorer 4.0.

Follow these instructions:

Internet Explorer 4.0: Select Internet Options (Under the view menu), and click on the "security tag." Under the Zone pull down

menu, select "Trusted sites zone." (The security level "Low" should be selected.) Click on "Add Sites," then type in "<http://umweb2.unitedmedia.com>" Uncheck "Require server verification (https:) for all sites in this zone."

Click "OK" twice.

Everybody out there who sets firewall security policy comfortable with that?

Mark Jackson - <http://www.alumni.caltech.edu/~mjackson>

Hacking, Irish-Style

"Fiachra O Marcaigh" <fiachra@iol.ie>

Tue, 29 Sep 1998 13:57:32 GMT

No backdoors or Trojans required for a four-man gang that wanted to

incapacitate the phone-monitored alarms in a rural area in the south of the

country. They busted in the door and took hammers to the exchange equipment,

in an attack that left 500 families without telephone service.

It is ironic that the provision of extra services such as alarm monitoring by the phone company has made its exchanges a target of attack. Perhaps they should install a decent alarm system?

Full story: <http://www.irish-times.com/irish-times/paper/1998/0929/hom16.html>

⚡ Re: X-rated net suit (PGN's comment in [RISKS-19.97](#))

"Rishiyur S. Nikhil" <r.s.nikhil@mediaone.net>

Fri, 25 Sep 1998 19:48:15 -0400

> [Combine digital photography with the see-through infrared camera
> technology described in [RISKS-19.93](#) and we get undie-lewded truth? PGN]

Beware of geeks baring gifs.

Rishiyur S. Nikhil (nikhil@acm.org)

⚡ Re: Sexy risks of searching for MP3 (Markowitz, [RISKS-19.97](#))

John Mee <jmee@ns.net>

Sat, 26 Sep 1998 08:33:01 -0700

In [RISKS-19.97](#), "Sidney Markowitz" <sidney@sidney.com> pointed out that a number of porn sites will add meta tags pointing to rock bands. In a recent investigation at my workplace, we (I work in Information Security) discovered that an alarmingly high number of the sites are using

www.disney.com as either a link or a meta tag so that children will find these sites when they go out and look for pictures of Mickey and Goofy. Parents would be well advised to check the global history and cache files of their browsers to see if this has happened and also have a talk with their children about things. My own son, while doing some research on the U.S. Govt. found out that Whitehouse.com does NOT contain government info :-)

Moral: Maintain open communication with your children and monitor their Web usage.

✂ Re: Sexy risks of searching for MP3 (Larry, [RISKS-19.97](#))

Don Byrd <dbyrd@cs.umass.edu>
Mon, 28 Sep 1998 11:48:03 -0400

[...] Actually, the Web-search companies are well aware of unscrupulous Webmasters trying to manipulate their search systems, and they have been taking countermeasures for quite a while. See for example the following discussion, at <http://searchenginewatch.com/webmasters/rank.html> :

Meta tags are what many web designers mistakenly assume are the "secret"

to propelling their web pages to the top of the rankings. HotBot and

Infoseek do give a slight boost to pages with keywords in their meta tags.

But Excite doesn't read them at all, and there are plenty of

examples

where pages without meta tags still get highly ranked. They can be part of the recipe, but they are not necessarily the secret ingredient.

Search engines may also penalize pages or exclude them from the index, if they detect search engine spamming. An example is when a word is repeated hundreds of times on a page in a row, to increase the frequency and propel the page higher in the listings. Search engines watch for common spamming methods in a variety of ways, not the least by following up on complaints.

I don't know that this description is totally accurate but I'm confident it's basically correct. And I have seen the ignoring-Meta effect. A while ago, one of my colleagues built a simple Web search system and used it to search for "biochemistry" (or some such, I'm not sure any more). One of the top hits was a university department page which neither used the word "biochemistry" heavily nor seemed particularly relevant to it; however, it did repeat the word numerous times in a META tag. But one of the well-known search services we tried (Alta Vista? Infoseek? I forget) was not fooled at all.

Don Byrd, Center for Intelligent Information Retrieval (CIIR),
Computer Sci.,
University of Mass., Amherst, MA 01003 1-413-545-3147 dbyrd@cs.
umass.edu

⚡ Y2K risk in Netscape cookies

<jseymour@a1.ibm.com>

Sat, 26 Sep 1998 00:58:13 +1000

How did the following happen?

The Netscape cookies specification (url below) states that the expires field of the cookie string is formatted as:

Wdy, DD-Mon-YY HH:MM:SS GMT

A 2 digit year! In a specification from circa 1994-95!! What planet am I on?!!!

More seriously, how many web applications will stop working around the year 2000 because of differing interpretations of what YY means?

<http://developer.netscape.com/docs/manuals/communicator/jsguide4/cookies.htm>

⚡ Re: "Windows NT Security" (Frankston, [RISKS-19.95](#))

Russ <Russ.Cooper@rc.on.ca>

Fri, 25 Sep 1998 15:30:57 -0400

First, Bob Frankston mentioned that Windows NT "has been C2 certified,"

Then, John Nolan said it was Windows NT 3.51.

Actually, it was Windows NT 3.5 (Workstation and Server) with Service Pack 3.

In <http://www.radium.ncsc.mil/tpep/epl/entries/CSC-EPL-95-003>.

[html](#)> the

NSA state that the highest level NT 3.5/SP3 could meet and satisfy all criteria is class C2.

- It's correct that the evaluated platforms were not networked.
- Extensive modifications were not made to the system registry (some were, but considering the size and scope of the registry the mods could not be called "extensive").
- Like all evaluations, it was done on specific hardware that was also specifically configured (sans floppy, for example). Compaq Intel and Dec Alpha configs were evaluated.

See <http://www.radium.ncsc.mil/tpep/process/procedures.html> if you're interested in the RAMP process.

MS went the ITSEC route with NT 3.51, and received an E3 assurance level in the U.K. in 1996 <<http://www.itsec.gov.uk/cgi-bin/cplview.pl?docno=27>>. From a marketing perspective, it was a better schpiel (NOS certification rather than OS), especially since they were already allowed to sell into the .gov/.mil by virtue of the NSA C2 evaluation on 3.5SP3 (which purchasing managers seem to gleefully ignore btw). Novell contends its not a "network" evaluation <<http://developer.novell.com/research/appnotes/1997/november/02/05.htm>>.

NT 4.0 (Workstation and Server) are under ITSEC E3,F-C2 functionality evaluation with AISEP (DSD Australia) <<http://www.dsd.gov.au/epl/os.html>> but have not, as far as I know,

completed it anywhere.

Personally, I think all of this evaluation junk (at this level) is just that. I feel much better passing an ISS scan or an Axent audit than I do knowing some pseudo-spooks had a gander at it. IMO, anything below B is intended to keep responses to RFPs to a minimum and make purchasing somewhat simpler.

Russ - NTBugtraq moderator

Join the NTBugtraq list, see <<http://ntbugtraq.ntadvice.com>>

✉ Re: "Windows NT security"

Joe Thompson <joe@orion-com.com>

Fri, 25 Sep 1998 23:48:27 -0400

There was a forum on InfoWorld Electric (<http://www.infoworld.com/>) about

this about a month or so ago. The actuality of NT's C2 certification is dependent on the following:

- * One of two or three (I seem to remember two Compaqs and one Digital system) very specifically detailed hardware configurations must be used.

These do not include any kind of external connectivity (network card, modem).

- * The version of NT that was certified was NT 3.5 with Service Pack 3 applied, and no networking or comm drivers installed. 3.51 is not certified, nor is 3.5 without SP3. 4.0 has not, to anyone's

knowledge,
began the process of certification, and Microsoft declined to
comment.

The forum was started by InfoWorld columnist Nicholas Petreley,
who spoke
with a fellow named Ed... I can't recall his last name, but he
headed up
Lone Star Systems, the company which developed the testing
software that
Microsoft used to gain the seal of approval. He alleges that
Microsoft has
both actively and passively misrepresented the security of NT
to, among
others, government agencies, and that Microsoft reneged on
promises to
distribute his compliance-testing software.

It was a very interesting forum. Petreley sent a comprehensive
list of
questions to Microsoft and their answer was a blanket "no
comment." Most
of the questions were not even speculative in nature, but were
seeking
comment on facts that could easily be verified independently (e.
g., details
about Microsoft displays at various trade shows).

Nicholas will be happy to comment I'm sure, and the forum
discussion should
still be archived (I'd provide direct addresses and URLs, but my
copy of
Netscape is flaky today). -- Joe

✉ Enquiry re: problems at universities

Pete Mellor <pm@csr.city.ac.uk>
Tue, 22 Sep 1998 10:48:43 +0100 (BST)

I am interested in any information regarding software disasters

that have
affected administrative systems in universities, such as student
records,
registration systems, etc.

These need not be recent. (In fact, my enquiry is prompted by an
acquaintance telling me that several incidents resulting in
permanent loss
of student records occurred back in the 1970's, when
universities were
either just getting computerised or else upgrading to new
mainframes.)

Please reply to me directly, rather than to RISKS. I will post a
summary of
any interesting incidents, unless the respondent indicates that
the
information is confidential, in which case I will treat it as
such.

Many thanks.

Peter Mellor, Centre for Software Reliability, City University,
Northampton
Square, London EC1V 0HB, UK. Tel: +44 (171) 477-8422, Fax: +44
(171) 477-8585
E-mail: p.mellor@csr.city.ac.uk

[For starters, a very cursory search of the RISKS archives
(for example, <ftp://ftp.sri.com/illustrative.ps> or [pdf](#))
found these
references to RISKS (R i j) and ACM SIGSOFT Softw.Eng.Notes
S (i j)
(with earlier references to RISKS):
Computer blunders blamed for \$650M student loan losses (S 14 2)
New Zealand student grants debited instead of credited (S 14 5)
Brown University senior's account mistakenly given \$25,000 (S
12 2)
Ontario removes privacy controls on students' personal
information ([R 19 48](#))
New computer system duns students for loans not due (S 18 2:9)
Univ. Central Florida did not cut off student registration (S
12 3)

On-line class registrations deleted by other students at UBC
(S 18 1:19)

``Computer error" affects hundreds of UK A-level exam results
([R 19 40](#))

British school examination program gave erroneous grades (S 11
5)

Computer gives law student wrong exam, passes him, after disk
fix (S 12 2)

16-year-old boy cracks university computer security (S 21 2:20)

Vandalism disrupts service at Stirling University for days (S
19 4:13)

PGN]

🔥 REVIEW: "Decrypted Secrets", F. L. Bauer

"Rob Slade" <rslade@sprint.ca>

Tue, 29 Sep 1998 10:32:31 -0800

BKDECSEC.RVW 980804

"Decrypted Secrets", F. L. Bauer, 1997, 3-540-60418-9, U\$39.95

%A F. L. Bauer

%C 175 Fifth Ave., New York, NY 10010

%D 1997

%G 3-540-60418-9

%I Springer-Verlag

%O U\$39.95 212-460-1500 800-777-4643

%P 447 p.

%T "Decrypted Secrets: Methods and Maxims of Cryptology"

Cryptology is the study of the technologies of taking plain,
readable

text, turning it into an incomprehensible mishmash, and then
recovering the initial information. There are two sides to this
study. Cryptography is the part that lets you garble something,
and

then recover it if you have the key. Cryptanalysis is usually
seen as

the "dark side" of the operation, because it is the attempt to

get at
the original meaning when you *don't* have the key. Most
current and
popular works on cryptology actually only speak about
cryptography.
For one thing, nobody wants to get into trouble by telling
people how
to break encryption. However, it is also much easier to
blithely talk
about key lengths and algorithms and pretend to know what you are
doing if you don't have to understand enough math to try to
figure out
how to go about cracking a particular cipher.

Bauer examines both sides, which is an important plus. If you
need to
decide how strong an encryption algorithm or system is, it is
important to know how difficult it might be to break it.

Chapter one looks at Steganography, the science of hiding in
plain
sight, or concealing the fact that a message exists at all. In
this
he first demonstrates a wide ranging historical background which
is
quite fascinating in its own right. Basic encryption concepts
are
introduced by the same historical background, but move on to a
very
dense mathematical discussion of cryptographic characteristics in
chapter two. Encryption functions are started in chapter three,
and
it is delightful to have examples other than Julius Caesar's
substitution code. Polygraphic substitutions are in chapter
four and
the math for advanced substitutions is in chapter five. Chapter
six
introduces transpositions. Families of alphabets, and rotor
encryptors such as ENIGMA, are reviewed in chapter seven. Keys
are
discussed in chapter eight, ending with a brief look at key
management. Chapter nine covers the combination of methods
resulting

in systems such as DES (Data Encryption Standard). The basics of public key encryption is introduced in chapter ten. The relative security of encryption is introduced in chapter eleven, leading to part two. However, it also ends with a discussion of cryptology and human rights, concentrating mainly, although not exclusively, on the US public policy debates.

Part two examines the limits of functions used in cryptography, and thus the points of attack on encryption systems. Chapter twelve calculates complexity, and thus the size of brute force attacks. Known plaintext attacks are the basis of chapters thirteen to fifteen, looking first at general patterns, then at probable words, and finally at frequencies. Frequency leads to a discussion of invariance in chapter sixteen. Chapter seventeen follows with a look at key periodicity. Alignment of alphabets is covered in chapter eighteen. Of course, cryptographic users sometimes make mistakes, and chapter nineteen reviews the different errors and various ways to take advantage of them. Chapter twenty one looks at anagrams as an effective attack on transposition ciphers. The concluding chapter muses on the relative effectiveness of attacks and of cryptanalysis overall.

Those seriously interested in cryptology will really need to be serious: brush up on your number theory if you want to use this book for anything. On the other hand, Bauer's history and vignettes from the story of codes and the codebreakers are interesting, amusing, and accessible to anyone.

copyright Robert M. Slade, 1998 BKDECSEC.RVW 980804



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 2

Saturday 3 October 1998

Contents

- [Risks of Upgrades: Florida fingerprint system](#)
[Charles P Schultz](#)
- [Bank error delays 50,000 Ontario social assistance payments](#)
[Mark Brader](#)
- [More --possibly unpublished-- banking/credit card failures](#)
[Luc Bauwens](#)
- [Attack on blood databases was simulated](#)
[Dorothy Denning](#)
- [JavaScript Flaw in Netscape](#)
[Edupage](#)
- [Not all outages are bugs: taxi credit](#)
[George Michaelson](#)
- [Y2K police planning](#)
[Alex Klaus](#)
- [Re: Win NT C2 Certification](#)
[pchallin](#)
- [Education and other undesirable numbers](#)
[David Collier-Brown](#)
- [Less sinister reason for Disney link in porn site](#)
[Andrew Klossner](#)

- [Re: Sexy risks of searching for MP3](#)
[Michael Smith](#)
 - [Re: Y2K risk in Netscape cookies](#)
[Jay Ball](#)
 - [Re: How to bypass those pesky firewalls](#)
[Brad Ackerman](#)
[Phillip C. Reed](#)
[Chris DeLashmutt](#)
 - [Information Security Educators Mailing List](#)
[Fred Cohen](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Risks of Upgrades: Florida fingerprint system

CharlesP Schultz-ECS013 <CharlesP_Schultz-ECS013@email.mot.com>

Thu, 1 Oct 1998 18:10:11 -0500

Computer Glitch Ties Up Crime Probes
from *The Palm Beach Post*, 1 Oct 1998,
Monika Gonzalez, Palm Beach Post Staff Writer

This article reports that "dozens of crimes in Palm Beach County could be going unsolved because the sheriff's computers can't compare fingerprints found at crime scenes with those of criminals arrested in other parts of the state."

The problem is a software compatibility problem that was caused by upgrades made to the network of state and local fingerprint computers know as AFIS - Automated Fingerprint Identification System. In 1996, the Palm Beach County Sheriff's Office and the Florida Department of Law Enforcement both decided to upgrade. Palm Beach finished their upgrade first, in October, 1996,

expecting to be compatible with the state's system about six months after that. However, the state upgraded their system beyond the capabilities of the county's upgrade, making them incompatible, and they remain so to this day. Mark McDonald, Palm Beach County AFIS Supervisor "hopes" the two systems can be compatible by January, 1999 after upgrading his system again. (This should give them about a year of full operation before the Y2K bug hits them! - but I digress...)

Losses:

Palm Beach County was getting two to three fingerprint matches a month from the state system. This comes to 48-72 cases that might be closed by now (2 years since October, 1996). Some of these matches may be discovered once the systems are linked again, but the statute of limitations may have run out on some of the crimes in question. Also, any belongings or evidence that might have been recovered because of a timely fingerprint match may be lost. This is exacerbated by the fact that Palm Beach County estimates it will take another year to process the fingerprint backlog.

Lessons:

- 1) Plan and coordinate your upgrades carefully
- 2) Come to Palm Beach County to commit your crimes before they can trace your fingerprints!

Charles P. Schultz <ecs013@email.mot.com>

⚡ Bank error delays 50,000 Ontario social assistance payments

Mark Brader <msb@sq.com>

Thu, 1 Oct 98 07:18:43 EDT

It isn't only Bank of Montreal customers who've been having trouble this week. Yesterday 50,000 Ontario social assistance (welfare) recipients who receive this payment by direct deposit to their Toronto-Dominion (TD) Bank accounts ... didn't.

This was the result of an error the day before. The Royal Bank of Canada actually deals with the provincial government on this, and they had prepared as usual a file of 50,000 deposits to transmit to the TD Bank at 4:30 pm the day before. However, this time the date codes on the file were wrong.

Someone at the Royal Bank soon noticed the error and called the TD Bank to notify them to expect a corrected file. This was transmitted, still in good time to be processed overnight as usual, but according to today's Toronto Star, "a technician forgot to manually let the computer know that a new file was in place."

The victims, of course, were precisely those people least able to cope with even a 24-hour delay in payment. They were basically thrown on the mercy of their individual branch staff, who might, or might not, issue emergency advances or provide overdraft protection.

The TD Bank is the fifth-largest in Canada; the Royal Bank is the largest.

--Mark Brader <msb@sq.com>

✈ More --possibly unpublished-- banking/credit card failures

"Luc Bauwens" <bauwens@ucalgary.ca>

Fri, 2 Oct 98 9:00:03 MDT

Apparently, on 16 Sep 1998, the entire Diner's Club authentication system in Belgium was off the air. (I tried using mine unsuccessfully that day, and I heard from another store, just before leaving on the following day, that indeed, their whole network had been out that day for most of the day.)

Then, back to Canada, on 30 Sep I received the following e-mail from our payroll people:

"We have been advised that there has been a failure in the transmission of payroll deposit data between the Royal Bank and the Toronto Dominion Bank. The result is that the U of C employees who are TD Bank customers did not have their funds deposited this morning. Our information is that the bank is moving quickly to resolve this problem and that the funds will be deposited no later than tomorrow morning. If you have any concerns, please contact your bank."

One wonders how common these types of occurrences are? And how often they remain unpublished?

Luc Bauwens, The University of Calgary, Mechanical and Manufacturing Eng.

Calgary AB T2N 1N4 Canada 1-403-220-5792 <http://www.acs.ucalgary.ca/~bauwens>

✶ Attack on blood databases was simulated (Re: [RISKS-19.97](#))

Dorothy Denning <denning@cs.georgetown.edu>

Fri, 2 Oct 1998 09:13:21 -0400

[(Correcting the record on Bob Brewin's previous article in *Federal Computer Week*, cited incompletely in [RISKS-19.97](#),) PGN]
According to a 30 Sep 1998 article by Bob Brewin in *Federal Computer Week*, the attacks on DoD medical databases previously described were simulated as part of a read team exercise. A Pentagon spokeswoman told FCW that the exercise was designed to "demonstrate potential impacts...if personnel records, such as medical records with information on blood types of military members, were the subject of hacker attacks." The woman said that "No records were electronically altered" during the exercise. Even then, the exercise was against an incomplete demonstration model of DOD's Defense Blood Standard System, which had been placed on the Web so that DOD users could look at the new system. In practice, the hospitals are said to operate stand-alone systems that are not connected to the Internet.

<http://www.fcw.com/pubs/fcw/1998/0921/web-blood-9-22-98.html>

Dorothy Denning

⚡ JavaScript Flaw in Netscape (Edupage)

Edupage Editors <educause@educause.unc.edu>

Tue, 29 Sep 1998

A computer consultant has identified a flaw in the Netscape browser that would allow a malicious programmer using JavaScript to read the contents of another user's cache (the temporary storage on a computer's hard drive), and thereby get access to the user's files. However, encrypted information, including credit card numbers, would not be vulnerable from this flaw, because they are not stored in cache. Emphasizing that the flaw is hypothetical and that no one has reported being affected by it so far, a Netscape executive says the company is taking immediate steps to verify and fix the problem. Industry analyst Stan Dolberg says that the next 18 to 24 months will amount to a normal "shakedown cruise" for e-commerce, and that "this kind of stress-testing is going to discover all kinds of flaws... Today, in and of itself, this particular flaw is not earthshattering." (*USA Today*, 28 Sep 1998; Edupage, 29 Sep 1998)

⚡ Not all outages are bugs: taxi credit

George Michaelson <ggm@dstc.edu.au>

Fri, 2 Oct 1998 16:51:56 +1000 (EST)

Lately, local taxis using automatic ATM cardswipe have been

falling back on manual payment. After the 20th time, I asked why, assuming it was bad reception which was known to plague the system early on. It turns out the taxi agency has given the card-processing agency 6 weeks to settle on card transactions. The drivers can convert paper-processed cards into cash immediately, at a small discount (they trade like funny money among the drivers, and small-shop owners and petrol stations) and really dislike having a 6 week wait for settlement on the electronic funds transfer. Plus, the cards incur a 3% process fee so the agency wins twice: once on the processing fee, once on the interest earned putting the money in play for a month or so.

I think this is a social RISK. The engineering decision to go cashless is fine, but the greedhead outcomes defeat things. Its still slow, its still manual, but the drivers just *prefer* it.

-George

⚡ Y2K police planning

Alex Klaus <alex.klaus@sympatico.ca>

Sat, 03 Oct 1998 10:28:07 -0400

The **Ottawa Citizen** (03 Oct 1998) reports that the RCMP has banned vacations for its 15,000 officers and 2,400 civilian members from Dec., 27, 1999 to March, 1, 2000. According to Dave Morreau, who heads the RCMP's Y2K

project the length of the ban was determined by the need to include " ... all the dates that computer experts say ill prepared computer systems would be likely to crash or malfunction." For its part, "... the force has already fixed and tested about 90 per cent of its systems ... " notes Morreau. Additionally the article also reports RCMP attempts to create an accurate picture of any potential Y2K problems are hindered by " ... many businesses and utilities ... reluctant to discuss whether their systems have been fixed for fear of facing [customer]lawsuits ..." In a memo to the force, Commissioner Murray noted the situation may be like last January's Ice Storm, which affected Eastern Ontario and Quebec with power outages etc. Though Murray does not expect problems throughout the whole period but " ... problems probably of a limited duration may occur." The last time such such an ban was issued the article notes, was during the Pope's 1984 Canadian visit. The full text of the article can be found at <http://www.ottawacitizen.com/national/981003/1910271.html>

[Though other police forces probably have these contingency plans in effect, it is interesting to see how the Y2K bug is becoming noticed in all quarters now.]

✉ Re: Win NT C2 Certification

<pchallin@bama.com>

Fri, 2 Oct 1998 10:22:17 -0500

I got the following from Paul Thurrott's "Wininfo" dlist for Oct 1, 1998 (<http://www.wugnet.com/wininfo>) regarding Windows NT C2 Certification

Quoting>>>

An update on Windows NT 4.0 and the C2 evaluation

Last week, I got a tremendous amount of information about C2 from various WinInfo readers and, originally, I had intended to publish most of it. But I just received an interesting post from Frank Mayer, of Science Applications Internal Corporation (SAIC), the company that Microsoft has contracted to get Windows NT 4.0 evaluated for the C2 rating. Frank is a a long-standing and well-respected member of the security community, which is one of the reasons SAIC was chosen to work with Microsoft on the NT 4.0 evaluation. I think I'll just present his own description of the status of Windows NT and C2, since he does sum it up quite nicely and probably understands the process better than most.

Here it is, only slightly edited for formatting.

There appears to be much confusion with regard to Windows NT and the status of its C2 evaluation. I'll attempt to set the record straight with the facts. My background with this topic runs from early in the evaluation efforts in 1992, where as a department director at The Aerospace Corporation, a federally funded research corporation, I was a member of the government C2 evaluation team for the original Windows NT

evaluation, to
today, where my organization at SAIC is conducting the current C2
evaluation.

Windows NT 3.5 was awarded a C2 rating in July 1995 (See this
Web page:

[http://www.radium.ncsc.mil/tpep/epl/entries/CSC-EPL-95-003.
html](http://www.radium.ncsc.mil/tpep/epl/entries/CSC-EPL-95-003.html)). This was a

stand-alone evaluation (i.e. no networking was evaluated). The C2
configuration did require some permissions within the file
system and

Registry to be changed from their out-of-the-box defaults (it is
well known

that the default permission settings in Windows NT are not
conservative from

a security perspective). Other configuration and Registry
settings were

also included as part of this evaluation, some optional (e.g.,
crash on

audit full) some not (e.g., "allocated" floppy and CD drive to
interactive

user). This is not atypical for C2 evaluated configurations.

As the Windows NT 3.5 evaluation was closing, discussions and
planning

between Microsoft and the government for a networked Windows NT
3.51 (later

4.0) evaluation were taking place. A team leader was assigned
and a team

formed. At this point (early 1996), I left Aerospace for SAIC
and so had

no direct knowledge for the next 9 months or so. In late 1996,
SAIC and

Microsoft began discussions about SAIC helping Microsoft move
forward with

the C2 evaluation of Windows NT 4.0.

In the summer of 1997, SAIC and Microsoft signed an agreement
whereby SAIC

would help Microsoft re-start the C2 evaluation efforts for
Windows NT 4.0

(See <http://www.cist.saic.com/nt.html>). Originally, we were to
help

Microsoft work with a government evaluation team to facilitate the evaluation. In early 1998, we transitioned the effort into an SAIC-staffed evaluation team under a government program that is commercializing the product evaluation program (See <http://www.radium.ncsc.mil/tpep/ttap/index.html>).

Our evaluation team has been working closely with Microsoft all year. A major milestone for this evaluation, the first of two government technical review boards (TRBs), will occur 29-30 September 1998. This TRB is NOT the point at which a "pass or fail" decision is made; rather it is intended to "ensure that the evaluation team has performed sufficient analysis of the product design" (See the "IPAR/Test Technical Review Board Meeting" section at <http://www.radium.ncsc.mil/tpep/ttap/Process.html>). So it is indeed true that Windows NT 4.0 has not completed a C2 evaluation for a network configuration. However, it is also true that significant effort is actively being directed towards that end, and the evaluation is well into the evaluation process. The targeted evaluation version (subject to changes) is Windows NT 4.0 with Service Pack 4 in a closed network configuration.

Finally, I'd like comment on C2. A "product" evaluation is a fairly in-depth (by today's standard) analysis of an operating system (or other type of technology) against a standard (e.g., C2). The C2 requirements are entirely contained on 3 pages of text. It takes a lot of interpretation and analysis to assess compliance of something as complex as an operating

system with something as simple as 3 pages of technical requirements. In order to keep the evaluation process tractable, an "evaluated configuration" is defined that scopes the evaluation effort. Rarely if ever would a C2 evaluated product be "rated" with all the functionality supported by that product or in its default configuration. This is OK and, I'll assert, even good. Because what a C2 product evaluation is intended to provide is assurance that, for the "evaluated configuration," a standard set of security features (e.g., access and security auditing) at a standard level of assurance (e.g., internal design analysis and security functional testing) is assessed by an independent third party at a level of detail more than product consumers could afford. A user/integrator would then take that product, understand it's "evaluated configuration," and use that as a starting point for building a secure system. Certainly everyone deviates from evaluated configurations. However, now they have the opportunity to start from an established and evaluated starting point.

Frank Mayer (mayerf@saic.com), Center for Information Security Technology,
Science Applications Internal Corporation

end quote >>>>>>>>

[By TODAY's standards, the Orange Book C2 criteria are extremely minimal, and a C2 evaluation should not be overendowed in any case. Indeed, the entire Orange Book evaluation criteria and the ensuing Rainbow series

interpretations leave many opportunities for vulnerabilities. For example, the Orange book says almost nothing about networking, which was relegated incompletely to the Red Book. For a discussion of some of the limitations, see my paper, Rainbows and Arrows: How the Security Criteria Address Computer Misuse ["Do Not" might appropriately have prefaced "Address" in the title], in the Proceedings of the 1990 NSA/NIST National Security Conference, and a later paper by Willis Ware, A Retrospective of the Criteria Movement, in the 1995 incarnation of the same conference. PGN]

✶ Education and other undesirable numbers

David Collier-Brown <davecb@Canada.Sun.COM>

Fri, 02 Oct 1998 14:56:59 -0400

In a discussion of the Ontario education number (briefly mentioned in [RISKS-19.48](#)), a quite unexpected risk raised its head.

A colleague had noted that ``the assignment of a number and collection of data can proceed without having to inform you'', which is a risk in itself, and speculated that a government might wish to apply an education number to anyone, to serve as the government's universal citizen identifier.

Alas, this turns out to be more than mere speculation: in Ontario, there is no particular interests in ever retiring any issued number: they persist

until the digits roll over to 0000000000 again.

This implies that any Ontario identifying number will be for life, and that universal ones like education numbers will be attached to all citizens within a generation, and finally that there will be no clashes with another person within one's lifetime.

No additional impropriety by a government is needed: all the components are already present.

You *will* be given a universal citizen identifier. It may be used for any purpose mentioned in the statute or in regulations subsequently made under it. It will not be subject to the Protection of Privacy act, and The information to be collected will be ``personal information'' which is defined to include such things as sexual orientation and political beliefs.

There is no particular reason to believe that Ontario is the only jurisdiction with numbers which persist in this manner, or with weak controls.

David Collier-Brown, 185 Ellerslie Ave., Willowdale, Ontario N2M 1Y3 CANADA
1-416-223-8968 | <http://java.science.yorku.ca/~davecb>
davecb@hobbes.ss.org

⚡ Less sinister reason for Disney link in porn site

Andrew Klossner <andrew@user2.teleport.com>
Fri, 02 Oct 1998 10:23:25 -0700

I believe the links to www.disney.com in porn web sites are for

the opt-out
doors. The usual first page presents buttons labeled "I am an
adult, let me
in" and "I don't want to see porn." Clicking the latter takes
you to
Disney's page. I think the resulting appearance of these sites,
when
searching for "disney," is unintended.

Andrew Klossner (andrew@teleport.com)

✉ Re: Sexy risks of searching for MP3 (Byrd, [RISKS-20.01](#))

Michael Smith <emmenjay@zip.com.au>

Sat, 03 Oct 1998 22:25:31 +1100

>[...] Actually, the Web-search companies are well aware of
unscrupulous
>Webmasters trying to manipulate their search systems, and they
have been
>taking countermeasures for quite a while.

There seems to have been an improvement here. Around 12 months
ago, while
doing some research I did a search on www.altavista.com for
someone who is
widely known in Australia. The search results consisted almost
entirely of
unrelated pornography sites. Having read Don Byrd's article, I
just
repeated the search on www.altavista.com and www.excite.com and
in the top
20 hits for each, there wasn't one irrelevant hit. (I didn't
look past the
top 20).

Michael Smith, Emmenjay Consulting Pty Ltd [http://www.zip.com.
au/~emmenjay/](http://www.zip.com.au/~emmenjay/)
emmenjay@zip.com.au

[Contribution edited by PGN]

✉ Re: Y2K risk in Netscape cookies (Seymour, [RISKS-20.01](#))

jay ball <jay@invengen.com>

Fri, 02 Oct 1998 09:38:35 -0400

> The Netscape cookies specification ...

> Wdy, DD-Mon-YY HH:MM:SS GMT

Well, in http://home.netscape.com/newsref/std/cookie_spec.html,
the

official cookie standard says: Wdy, DD-Mon-YYYY HH:MM:SS GMT.

the url

which you referred is the 'how to implement cookies with java
script'

page. i'll trust the standard.

i trust the standard to all ends, even the examples at the
bottom of the
page, with the demo of "09-Nov-99".

consistency.

jay ball <http://www.invengen.com> [one of several
contributions... PGN]

✉ Re: How to bypass those pesky firewalls (Jackson, [RISKS-20.01](#))

Brad Ackerman <bsa3@cornell.edu>

Fri, 2 Oct 1998 00:24:24 -0400 (EDT)

Turns out it's just checking for a recent version of Netscape
or Internet

Exploder. The applet liked the Power Macintosh G3 I'm typing this on once I downloaded the former.

In bloating the applet to qualify for the Intel program, United Media went a bit too far -- I'd call the minimum recommended platform an RS/6000 SP POWER2SC wide node, and I wish I were exaggerating. I'd recommend two towers of them (16 nodes) with the high-performance switch, but AFAIK no JVM would know how to distribute the processor load over multiple nodes.

The RISK of this sort of thing is crummy Java applets and other bloatware monopolizing USD 2e5+ computer equipment. Our interactive login nodes are crowded enough as is! [Yeah, there are processor quotas, but they can take a few days to update -- the system really doesn't protect all that well against UHF bogon emitters.]

Brad Ackerman, Cornell Theory Center

⚡ Re: How to bypass those pesky firewalls (Jackson, [RISKS-20.01](#))

"Phillip C. Reed" <reedpc@libbey.com>
Fri, 02 Oct 1998 08:02:51 -0400

I have to say that it's a poorly designed security structure that can be bypassed by doing ANYTHING to an inside client. If somebody on our net messes with their browser settings, the best they can expect is that their

access remains unchanged. More likely, the browser will fail to connect to the Internet at all.

Security controls must remain under control. Pretty much by definition, if you've put a client on somebody's desktop, you've lost (some) control of it, at least given today's operating system environment. Thus, the network security must **not** depend on the client.

phil reed, libbey inc. reedpc@libbey.com

✶ Re: How to bypass those pesky firewalls (Jackson, [RISKS-20.01](#))

Chris DeLashmutt <cdelashm@geocities.com>
Fri, 02 Oct 1998 10:03:49 -0400

First, Internet Explorer can (and should) be set up in such a way that users don't have access to change those kinds of security parameters. A small administrative task can help to slightly lower the risks of using the Internet.

Second, companies shouldn't just allow free reign to every site on the internet. Our location (only about 200 people) has implemented a pretty good method of limiting access to sites from our internal network. We actually disallow all but a few select sites for our people to get to on the web through our proxy server. Tyrannical as it may seem, it does work pretty well. The administration required at the startup was

pretty high in the beginning, but it is seldom that we have to change the allowances.

Finally, I think relying on a piece of application software, like a web browser, to handle your internet security seems like a pretty risky venture. Firewalls are generally single point software/hardware solutions that block access at the network layer (OSI model). It seems to me that the application-layer security features in Internet Explorer are meant more as an augmentation or refinement to the lower level security provided by a "Firewall".

Summary

Any serious approach to Internet security has to be comprehensive.

--Microsoft White Paper: Internet Explorer Security.

<http://www.microsoft.com/windows/ie/security/ie4security.htm>

September 16, 1998

Information Security Educators Mailing List

Fred Cohen <fc@all.net>

Sun, 27 Sep 1998 11:34:23 -0700 (PDT)

Introducing:

The Information Security Educators Mailing List

secedu@all.net

Our mission is to provide an open forum for educators in information security to discuss issues related to courses, curriculum, books, and other education-related items. It is also a forum to allow

vendors and providers of educational materials to provide information (but not advertisements) to educators and a forum for those educators to discuss those materials.

List Rules:

Rule 1: The mailing list is fully moderated. Mailings are sent out no more than once per day, often not for several days, and sometimes it takes even longer. Submissions may be edited for size, to remove garbage in headings, excessive signature lines, and so forth.

Rule 2: You can sign up or off the list in the same way as you make submissions to the list. Because we are fully moderated, it all goes to the same place anyway.

Rule 3: Be polite and respectful or it won't be published.

To submit, sign-up, or remove email to:

secedu@all.net

The mailing list's Web page is:

<http://all.net/edu/index.html>

I try to find interesting pointers for my readers and place them here. If you would like to add a pointer to your Web page, submit it to the list and we will consider your submission.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 3

Tuesday 13 October 1998

Contents

- [Computerized gas-pump cheat](#)
[Conrad Heiney](#)
- [Trojan Horse infests 15,000 Internet chat users](#)
[Monty Solomon](#)
- [Computer glitch trips up Dow Jones industrial average](#)
[Cliff Sojourner](#)
- [IE4 and its "magical" features](#)
[Chenxi Wang](#)
- [Unreliable reception of e-mailed WP documents](#)
[Daniel P. B. Smith](#)
- [Microsoft web site denies access based upon Windows regional settings](#)
[Eric Ulevik](#)
- [Risks of installing Microsoft's Media Player](#)
[Wade Ripkowski via James Love](#)
- [Insidious SQL interpreter bug messes up files](#)
[David Tonhofer](#)
- [Netscape Netcenter password hint](#)
[Dan Pritts](#)
- [Radio clock blows daylight savings](#)
[Ian Macky](#)

- [The risks of "keep it simple" \[Martin D Kealey\]](#)
 - [Finland: Fraud with copied banking cards](#)
[Kimmo Ketolainen](#)
 - [Offensive information warfare deemed offensive?](#)
[PGN](#)
 - [Hackers stay a step ahead of China's cyber-police](#)
[PGN](#)
 - [LA 911 outage...backup worked!](#)
[Thomas Maufer](#)
 - [Some good Y2K news: whisky will be on tap for Hogmanay 1999](#)
[Declan McCullagh](#)
 - [Military preparations to mobilize for Y2K](#)
[Declan McCullagh](#)
 - [Void where prohibited by date](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Computerized gas-pump cheat**

"Conrad Heiney" <conrad@universityaccess.com>

Fri, 9 Oct 1998 12:55:06 -0700

Today's *Los Angeles Times* reports that the county district attorney has filed charges against four men who are alleged to have replaced computer chips in electronic gas pumps, thus cheating customers of between 7%-25% of their gasoline.

The url to the full story is

<http://www.latimes.com/HOME/NEWS/METRO/t000091711.html>

According to the story, the problem was hard to detect partly because the chips were programmed to generate accurate results in the five- and

ten-gallon amounts used for testing the accuracy of pumps.

The RISK here is twofold: That misplaced trust in digital technology can lead consumers not to check things like gas pumps, and that it's easier to fool the regulators with an intelligently programmed cheat.

Conrad Heiney conrad@universityaccess.com Manager, Systems & Development
University Access, Inc. <http://www.universityaccess.com>

[Also noted by David Leshner, heard on NPR, and Richard Schroepel. PGN]

⚡ Trojan Horse infests 15,000 Internet chat users

Monty Solomon <monty@roscom.com>

Fri, 9 Oct 1998 01:22:14 -0400

Due to a Trojan horse on Internet Relay Chat, Back Orifice (see [RISKS-19.90](#))

was apparently made available to up to 15,000 IRC users who transferred

files. This was discovered by GeoCities when it received thousands of

requests for the nfo.zip file. [Source: Trojan Horse Infests 15,000

Internet Chat Users, By Andy Patrizio, TechWeb, 8 Oct 1998, <http://www.techweb.com/wire/story/TWB19981008S0019>]

⚡ Computer glitch trips up Dow Jones industrial average

Cliff Sojourner <cls@cisco.com>

Thu, 08 Oct 1998 12:02:46 -0700

The Dow Jones Industrial Average was erroneous for the first 12 minutes Thursday morning 8 Oct 1998, resulting from the merger of, with the resulting Citigroup using Citicorp's ticker symbol, CCI. The previous night's closing price of Citicorp (in the \$70s) was used instead of the Citigroup opening price (31.75). [Source: Computer glitch trips up Dow Jones industrial average, By Margaret Kane, ZDNet, 8 Oct 1998; PGN Abstracting]

Cliff Sojourner, Cisco Systems Inc. cls@cisco.com
(408) 527-7637 170 W. Tasman Drive, SJ CA 95134 bldg H2/cube E2-7

[Also noted by Doneel Edelson]

⚡ IE4 and its "magical" features

Chenxi Wang <cw2e@cs.virginia.edu>
Mon, 12 Oct 1998 10:25:34 -0400

Last week my Windows 95 machine refused to boot, citing a protection error in the IO unit. My system staff, after laboring over my machine for some time, told me that it was due to a bug in the IO, and that according to Microsoft, the only way to fix it was to install IE4! So IE4 was installed, and sure enough, it fixed whatever problem the machine was having. I was doing some disk cleaning up this past weekend, and I accidentally deleted some files that appeared to have been installed by the IE installation. Curious to see if IE still worked, I double clicked on the icon. Guess

what

happened? -- It launched my netscape communicator to the URL of the IE download site! I was incredulous...

Chenxi Wang University of Virginia <cw2e@cs.virginia.edu>

✶ Unreliable reception of e-mailed WP documents

"Daniel P. B. Smith" <dpbsmith@world.std.com>

Fri, 9 Oct 1998 09:55:45 -0400 (EDT)

Some unpleasantness occurred in a meeting recently. Person A said that the reasons he hadn't performed a task was because he was still waiting for Person B to supply some needed information. Person B said he'd supplied it a week ago in a specific memo which he'd distributed via e-mail. Person C said, "I got it and I'm almost sure I saw A on the distribution list." Person A said "I got the earlier version where all of those numbers were blank, but I've never gotten anything that had the numbers." Person B said "What version where the numbers were blank?" Person E said "You know, the one you sent out about a week ago. I never got the one with the numbers filled in, either."

On comparing notes, it turned out that a single version of the memo had been e-mailed, and when opened by about half the participants a critical table was complete and had information visible in all columns, and about half of them had a column in which all cells were blank. All recipients of the damaged

version had simply assumed that the blank cells were intentional.

Incidentally, this was a 100%-pure-Microsoft situation, involving no version of Word more than a year old (no version skew of more than one version) and involved RTF format which is the format Microsoft specifically designates for document transfer. There was no obvious pattern to the problem; the originator used Word 97 on a PC, and some receivers using Word 98 on a Mac received it correctly while some receivers using Word 97 on a PC got blank columns. We don't know the full story but it is suspected that the set of fonts installed, the OS version, the screen dimensions and resolution, and the kind of printer the user is connected to may all play some part in this crazy equation.

The RISK here is the same as with any other kind of unreliable communication that is falsely assumed to be reliable. Notice that, in general, when you send a word-processing document to someone else, the sender has no reliable way to confirm what the receiver will ultimately see and print. Unless the user guesses there is something wrong and complains, the problem is likely to go undetected. Even when the problem is detected, it is usually hard to resolve, because nothing in the system logs all the configuration information that would be needed to resolve it. Unless the recipient is a colleague in an adjacent cubicle and is willing to experiment with you in real time, problems of this kind are likely to remain unsolved.

Daniel P. B. Smith <dpbsmith@world.std.com>

⚡ Microsoft web site denies access based upon Windows regional settings

"Eric Ulevik" <eau@astsun.fujitsu.com.au>

Tue, 6 Oct 1998 18:59:44 +1000

I use home.microsoft.com as my home page under Internet Explorer 4.01 SP1 running on Windows NT 4.0. I have customized the data; I like the presentation.

Today, I found that I can no longer access my home page. The browser is redirected to ninemsn.com.au - a local web site put together by Microsoft and Channel 9 (an Australian TV station). ninemsn tells me that this is "MSN strategy".

But other PCs in the same office are not redirected. The significant difference appears to be that the other PCs are set to US date formats.

The risk is that configuring your computer's date format has surprising consequences.

Eric Ulevik <eau@ozemail.com.au>

⚡ Risks of installing Microsoft's Media Player

James Love <love@cptech.org>

Sat, 03 Oct 1998 17:21:44 -0400

James Love, Consumer Project on Technology, P.O.Box 19367,

Washington, DC 20036

<http://www.cptech.org> love@cptech.org 202.387.8030, fax
202.234.5176

<--begin message from Wade Ripkowski-->

Subject: RE: Sony PC & Windows 98 Licensing
Date: Fri, 2 Oct 1998 14:21:23 -0400
From: "Ripkowski, Wade" <Wade.Ripkowski@psc.BellHowell.com>
To: "'James Love'" <love@cptech.org>

I just hate being abused by Microsoft. I just encountered a whole new issue with Microsoft's "new" Media Player that you may be interested in as well. I installed it and it changed EVERY multi-media association on the machine to use itself as the player. The problem here is that the media player I was using up until then utilized the hardware based MPEG decoder and subsequently played MPEG video better (no jumping). MS Media Player also redirected the CD Audio player to itself. Again the audio player I used before was much better.

To make a long story short. I opted to "uninstall" it think my system would be put back the way it was. Boy was I wrong. It uninstalled itself and changed all the multi-media associations to use Microsoft ActiveMovie! Now I am left with a system in which I must reinstall the Audio/Video applications I want in order to use them, and to top it off, my RealAudio player no longer works either! I spoke with a friend of mine this morning and he ran into the exact same problem I did, although he has a Gateway machine.

I think this is somewhat along the lines of the "browser

battle". It looks as if Microsoft knows they lost the battle, but if they can't own that, then they will own the multi-media portion of the machine. They advertise "forget all the plug-ins, all media, one player". So I should have read the literal meaning -- my mistake. And they are dumping this product free to everyone on the internet. This will surely hurt Real, Inc., and possibly other similar companies.

I am not opposed to one vendor writing all the software for the PC I use, if that software works properly and at an acceptable performance level. If one vendor wants all the business, fine, make software that earns it on merit, not on price / availability!!! [...]

<--end message from Wade Ripkowski-->

⚡ Insidious SQL interpreter bug messes up files

<David_Tonhofer@ept.lu>

Tue, 13 Oct 1998 12:08:56 +0200

Recently, the informatics department of our company found out - quite by accident - that the SQL interpreter on our midrange server (made by a well-known manufacturer) exhibited an interesting bug - in interactive and dynamic/compiled-in SQL queries.

An UPDATE query with an assignment of a constant value to a numeric field 'a' set 'a' field to '0' in case of a simultaneous assignment with any

field

on the right-hand side of that assignment and a 'WHERE'-condition, like so:

```
UPDATE table SET a = 10, b = b+b WHERE c > 10
```

resulted in 'a' having value 0 for all $c > 10$, whereas

```
UPDATE table SET a = 10.0, b = b+b WHERE c > 10
```

succeeded. Yuck!

With a bug like this, your company database might slowly turn belly-up without anyone noticing.

Anyway, after the manufacturer's help-desk had analyzed the problem, we applied patch SF47057 and everything was well ever after (we hope).

Risk: Do not forget to apply your patches. Also, the system your are building on or upgrading to might be flakier than you thought.

-- DaTo

Netscape Netcenter password hint

Dan Pritts <danno@us.itd.umich.edu>

Mon, 12 Oct 1998 16:02:36 -0400

My Netscape is part of Netscape Netcenter, the service that Netscape is pushing as its entry to the Net portal business. My Netscape has, like most such services, a new account sign-up form.

This form is available via a 320+char URL which i have omitted for the sake of buggy mailers, and via the red "personalize" button in the upper left corner of <http://my.netscape.com/> (presumably only if you aren't already a member).

On this (non-encrypted) page, next to a field labeled "Enter a password hint:", you're given the following explanation of a password hint:

If you forget your password, Netcenter will present you this password hint to help jog your memory. Example hint:"same password as my bank acct."

The risks are obvious.

Amusingly, my initial attempt to send this report to Netscape failed; the "Feedback" link at the top of the same page is broken.

danno dan pritts

⚡ Radio clock blows daylight savings

Ian Macky <imacky@us.oracle.com>

Thu, 8 Oct 98 16:21:25 PDT

For the first time in many years I foolishly purchased a new high-tech consumer product: a clock with built-in radio receiver which listens to broadcast time standard and keeps synchronized. It's been accurate to the second since I turned it on... until last week, when one morning it was

exactly one hour early. It ended daylight savings time too soon!

Naturally, you can't force this clock in any way. You can't set the time, or change whether it honors daylight savings. You're at the mercy of a distant radio transmitter.

KISS! I should have known better. It's too bad noone is manufacturing any of Harrison's old designs (has everyone read "Longitude"?).

--ian

⚡ The risks of "keep it simple" [Re: Cohen, [RISKS-20.02](#)]

Martin D Kealey <martin@kurahaupo.gen.nz>

Mon, 05 Oct 1998 12:40:46 +1300

Sometimes simplicity can be deceptive; once again an example of making a simple stand-alone system in the present, without considering how it shifts complexity into other systems, either now or in the future.

Fred Cohen wrote:

> Rule 2: You can sign up or off the list in the same way as you
> make submissions to the list.

With respect, I'd like to suggest this isn't such a good idea.

> Because we are fully moderated, it all goes to the same place anyway.

In short, this is a non-sequitur, and irrelevant from the list subscribers' point of view...

It is always possible to start with multiple addresses aliased together;
it's a lot harder to start with one address and later get everyone out there to stop using it for everything, especially as most of the people you would want to stop will be people you've never heard from before (new subscribers) and therefore won't have had the chance to tell them that it's changed.
It's very difficult to un-make an omelet.

At some point in the future you may wish to revise your configuration; there are many reasons why it might need to be changed, but, for example, you may wish to have multiple moderators, while keeping list management under the control of a smaller group (even just one person). When that happens, it will be a lot easier to maintain the list with separate addresses for the separate functions.

As a secondary effect, not publishing such a standard address indirectly impacts on other mailing lists -- which necessarily may have separate addresses for some or all of submissions, subscriptions, administration, anonymizing, accounting and transport -- by not discouraging people from sending requests to the submissions addresses.

Not everyone running a mailing list has the time or dedication to hand-moderate everything, so I'd rather not encourage newcomers to make random broadcasts; "please add me to your list" gets to be quite an irritation to subscribers who are quite unable to do anything about it, while the list maintainer won't even see such a request unless they read (or

moderate) the list.

-Martin

🔥 Finland: Fraud with copied banking cards

Kimmo Ketolainen +358 40 55555 08 <kk@sci.fi>

Thu, 8 Oct 1998 07:47:27 +0300 (EET DST)

Someone apparently succeeded last Saturday in the old trick of copying banking cards' magnetic stripes and reading then the PIN codes from the keypad over the shoulder. What makes this scam spectacular is that the artist(s) had attached an additional "small black" card reader on top of the opening of the real reader in the cash dispenser.

They managed emptying some 60 accounts worth roughly 180 000 FIM (36 600 USD). In all, 500 customers have to renew their cards after using that particular cash dispenser on Aleksanterinkatu in Helsinki during the evening. No one has been arrested yet.

The three largest banks started to issue banking cards with a chip on top last year, but all cards still come with a magnetic stripe as well. Using a banking card in the chip card slot instead of the other one would have prevented this type of attack.

Kimmo Ketolainen, Finland <kk@sci.fi> <iki.fi/kk> +358 40 55555 08

[GREAT address: sci.fi! PGN]

⚡ Offensive information warfare deemed offensive?

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

Tue, 13 Oct 1998 7:12:13 PDT

``Hackers calling themselves the Electronic Disruption Theater allege the Pentagon used illegal offensive information warfare techniques -- a charge DoD officials deny -- to thwart the group's recent computer attack. At issue is whether in fighting back against the hackers, the Pentagon crossed the line into so-called offensive information warfare, and perhaps violated US laws that prohibit anyone from covertly accessing another's computer. The issue of computer crimes, however, is highly controversial because US legislation has not kept up with the capabilities of computer technology.''

This arose after a 9 Sep 1998 attack against DefenseLink, DoD's primary public information Internet site. The Pentagon apparently created Java applet (``Hostile Applet'') that shut down targeted browsers of hackers contributing to the collaborative attack. [Source: Hackers take offense at Pentagon defense; Experts Say DoD response treads fine legal line, *Defense News*, By George L. Seffers, 7 Oct 1998; PGN Very Stark Abstracting]

⚡ Hackers stay a step ahead of China's cyber-police

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

Tue, 13 Oct 98 5:52:01 PDT

Computer crime is increasing in China, with more than 100 cases in the past two years, one involving theft of \$1.2M. As a result, China is ratcheting up its Internet police and surveillance capabilities. Previous efforts have concerned pornography and undesirable political messages. Penetrations are now illegal, subject to up to five-year sentences. [Source: *People's Daily*, via Reuters News Service, 12 Oct 1998; PGN Abstracting]

⚡ LA 911 outage...backup worked!

Thomas Maufer <tmaufer@acm.org>

Mon, 12 Oct 1998 13:37:44 -0700

Wow, a backup system that actually worked. Of course, if the 911 system had had more than one source of electrical power, the backup might never have needed to be activated. Tom

<<http://dailynews.yahoo.com/headlines/local/state/california/>>

>L.A.'s 911 Goes Out For 17 Hours - (LOS ANGELES) -- Los Angeles police
>are pleased their 911 backup system works...following a 17-hour
>breakdown in the 911 system. Not a single emergency call was lost
>during the switch-over. The emergency system was knocked out during a
>fire in an underground storage area at City Hall on Saturday afternoon,
>when water from the sprinklers seeped into the electrical

system below.

>Authorities shut down power to the system, and the backup system kicked

>in...re-routing all calls to either individual police stations or the

>California Highway Patrol. The fire began in some unstable, illegal

>fireworks being kept for an investigation.

✶ Some good Y2K news: whisky will be on tap for Hogmanay 1999

Declan McCullagh <declan@well.com>

Fri, 25 Sep 1998 06:13:45 -0700 (PDT)

<http://www.scotsman.com/interactive/it16nips980923.1.html>

Distiller is 100% millennium proof

Whisky drinkers should be assured of their tipples being on tap for

Hogmanay 1999, says Alan Crawford

Whisky tipplers can rest easy after the announcement last week that a

technological crisis that had threatened to halt the flow of Scotch has been

narrowly averted. Burn Stewart Distillers, whose brands include Tobermory

Single Malt and Wallace Liqueur, has declared that its computer systems will

be millennium compliant by the end of the year.

Although the whisky industry is steeped in tradition, it relies heavily on

computers to control many aspects of production and marketing.

Burn Stewart

alone sells about 18 million bottles a year to 500 major customers. Failure

to deal with the millennium bug - which threatens global

computer meltdown
due to an inability to recognise the date change from 1999 to
2000 - could
result in widespread disruption of the distilling, bottling and
marketing
processes. [...]

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/>

✶ Military preparations to mobilize for Y2K

Declan McCullagh <declan@well.com>
Sat, 10 Oct 1998 14:30:52 -0700 (PDT)

[Declan notes that the Wisconsin National Guard is preparing to
mobilize
for Y2K <http://www.jsonline.com/news/1007y2k.asp>, as are Toronto-
area army
reservists, considering stockpiling food and generators. 2000
cyberglitch
the major concern for Canadian forces, By Patrick Cain]

✶ Void where prohibited by date

Rob Slade <rslade@sprint.ca>
Wed, 7 Oct 1998 14:48:02 -0800

Yesterday my wife brought home a copy of a letter that her
organization had
received from their insurance broker. As could be expected,
this document,

produced by the Insurance Bureau of Canada, warns that insurance is probably not going to pay out if something happens that is related to a Y2K bug. (They use more words to say it, of course.)

The pamphlet warns about a number of things that should be checked, and could be used to generate a reasonable list of items to be confirmed. Unfortunately, how you might go about checking them isn't covered. (There is one sidebar on checking the BIOS clock for a PC.)

However, that wasn't all that came in the mail yesterday. There was a catalogue from a company that sells promotional material related specifically to anniversaries. With it was a covering letter congratulating them on their tenth year in business, coming up this spring.

The institution my wife works for was founded in 1889.

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>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 4

Weds 21 October 1998

Contents

- [The risks of elbows on the French futures exchange](#)
[Steve Bellovin](#)
- [Electromagnetic interference on defense systems](#)
[PGN](#)
- [Wrong result in German Bundestag elections due to FAX machine](#)
[Harald Kucharek](#)
- [Emissions software glitch fails hundreds of older cars in Atlanta](#)
[J Quinby](#)
- [Another wild bank saga, from England](#)
[PGN](#)
- [AOL bytes the dust](#)
[PGN](#)
- [SRI voice-mail woes](#)
[PGN](#)
- [Re: Risks of installing Microsoft's Media Player](#)
[Michael F. Hogsett](#)
- [Software dictates names](#)
[Ruth Milner](#)
- [REVIEW: "Personal Encryption Clearly Explained", Pete Loshin](#)
[Rob Slade](#)

● [Dependable Computing for Critical Applications: CFP](#)

[Chuck Weinstock](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ The risks of elbows on the French futures exchange

Steve Bellovin <smb@research.att.com>

Fri, 16 Oct 1998 09:10:22 -0400

It turns out that elbows and computer keyboards don't get along. No, I'm not talking about RSI problems; rather, I'm talking about what can happen when an errant elbow hits a too-powerful key...

According to the 16 Oct **Wall Street Journal**, a trader at a French futures exchange accidentally leaned on his keyboard. Without realizing it, he placed an order to sell 14,500 government bond contracts, which caused the price to drop. His firm ended up losing several million dollars.

[I received reports on this from many of you, with 145 separate sell orders resulting from the trader leaning on the "Instant Sell" key.

Of course, in that "elbow" in French is "coude" (pronounced monosyllabically as "cooed"), it is clear that the futures exchange was

"couped" (also pronounced cooed), the victim of a coude coup! Next it

will be a little bird instead of an elbow, and we'll watch out for the

"cuckoo coup". TNX. PGN]

⚡ Electromagnetic interference on defense systems

"Peter G. Neumann" <Neumann@CSL.sri.com>

Tue, 27 Oct 1998 13:12:09 -0400

Patriot defenses and Predator unmanned aerial vehicles reportedly cannot work properly in certain foreign countries (Germany, Japan, South Korea and Bahrain are particular instances) because of frequency clashes. For example, Patriot missile system radios, radars, and data-link terminals clash with Korean cellular phones; U.S. force pages clash with Japanese aeronautical systems; crib monitors used on U.S. bases clash with German telephone service. In Bahrain, SPS-40 and SPS-49 radars are unusable because of interference from the national telecommunications services. (See the *Defense Week* issue that came out on 26 October 1998. Thanks to pwalczak@emh3.arl.mil (Paul Walczak) for pointing out this article.

[Also see <http://www.cnn.com/US/9810/17/pentagon.waves.ap/>

"At least 89 telecommunications systems ... were deployed within the

European, Pacific and Southwest Asian theaters without the proper

frequency certification and host-nation approval."

as noted by Roy Rodenstein, royrod@media.mit.edu, who reminds us of the

HDTV interference with Baylor hospital equipment ([RISKS-19.62](#)), and

points out that quasi-ad-hoc spectrum use must be stemmed in the

light of ever increasing uses of the spectrum.]

[For background, see my Illustrative Risks compendium, which now

provides an explicit descriptor (M) for the many cases of

interference

included therein:

<http://www.csl.sri.com/~neumann/illustrative.ps> or .

pdf ... PGN]

⚡ Wrong result in German Bundestag elections due to FAX machine

"Harald Kucharek" <harald.kucharek@realax.com>

Wed, 14 Oct 1998 17:54:02 +0100

The result of the elections to the German Bundestag has to be changed two weeks after the elections. The liberal FDP will loose one seat, the PDS will gain one. In the federal country of Brandenburg, the results were printed out double sided and then faxed to Bonn without taking into account that a fax only sends one side of a page.

⚡ Emissions software glitch fails hundreds of older cars in Atlanta

<jquinby@s1.com>

Mon, 19 Oct 1998 17:26:39 -0400

Due to a software glitch, hundreds of older cars in metropolitan Atlanta have failed emissions tests they should have passed. The state Environmental Protection Division allowed testing stations to keep flunking cars, even after EPD knew that the software thresholds in the ESP systems were a factor of two too low. [Source: the Georgia News section

of Yahoo's

News areas on 16 Oct 1998, and in the *Atlanta Journal and
Constitution*,

[http://dailynews.yahoo.com/headlines/local/state/georgia/story.
html?s=v/rs/](http://dailynews.yahoo.com/headlines/local/state/georgia/story.html?s=v/rs/)

19981016/ga/index_2.html#1 . PGN Abstracting]

⚡ Another wild bank saga, from England

"Peter G. Neumann" <Neumann@CSL.sri.com>

Wed, 14 Oct 1998 16:06:56 -0700

British Aerobics instructor Liz Seymour thought she might have
overdrawn her
bank account when she returned from vacation, but her bank
statement claimed
she was 121 billion pounds (British) overdrawn. That's 121
trillion pounds
by American counting, because the British billion is a million
million. The
bank also notified her she would be charged 2.5 (British)
billion pounds per
day in interest. When questioned, the bank chalked it up to a
typing error.

[Source: 14 Oct 1998, *Yorkshire Evening Press*]

[FOLLOW-UP CORRECTION in [RISKS-20.05](#). British Billion now US
also. PGN]

⚡ AOL bytes the dest

<PGN>

Mon, 19 Oct 1998 08:28:58 EDT

Someone masquerading as an AOL official sent e-mail to Network
Solutions

Inc. to change the aol.com domain-name entry on 16 Oct 1998. This request took effect automatically, because AOL was using lowest-level security (presumably not requiring manual intervention). As a result, AOL was effectively off the Net for incoming e-mail and Web use for about 12 hours.
[Source: Bloomberg News, 17 Oct 1998]

✶ SRI voice-mail woes

"Peter G. Neumann" <Neumann@CSL.sri.com>
Mon, 19 Oct 1998 10:14:35 -0700 (PDT)

I was away the past two weeks (although I did manage to put out one issue of RISKS on the fly). However, SRI's voice-mail system was not operational for something like five days last week. This is tough on incoming callers, but even tougher on travelers like me who try to keep in touch. The problem initially was attributed to bad sectors on one of the four hard drives. Further diagnostics identified a possible fault in the link between the PBX and voice-mail. The absence of both voice-mail and call-forwarding certainly makes life tough.

✶ Re: Risks of installing Microsoft's Media Player (Love, [RISKS-20.03](#))

"Michael F. Hogsett" <hogsett@csl.sri.com>

Tue, 20 Oct 1998 16:32:08 -0700

The thing that I find interesting here is that Apple addressed this kind of issue back in the mid 80's on the Macintosh. Each file has a four-letter creator (application) code and a four-letter file-type code. This allows multiple applications to be associated with the same file-type, since the Mac uses both to determine which application to load when the file is double-clicked as well as which icon to display in the gui for this file.

The creator and file-type codes are not limited to only letters. They can be nearly any character, essentially they are both simply 32-bit values. This allows for quite a few more file-types (and creators) than are allowed with the DOS/Windows 3-letter file types.

Michael F. Hogsett

[And software librarians will note that MS also subscribes to the GUI Guessimal System. PGN]

⚡ Software dictates names

Ruth Milner <rmilner@aac.nrao.edu>

Tue, 20 Oct 1998 11:44:03 -0600 (MDT)

Late last year, when I renewed my license, I learned that the New Mexico Motor Vehicles Division had gone to a new computer system. How did I find out? They issued my license in the name of "MRUTH MILNER".

I'm among the significant minority of people who use their given names in some way other than first-name-middle-initial. During a lengthy (and quite reasonable) discussion with someone fairly high up in the MVD, I learned that the states are under some federal mandate to make their driver databases interoperate. This is a very sensible thing to do, but in order to simplify the effort, they have apparently put some rather simpleminded restrictions on the name formats that are allowed.

1. Initial(s) and last name.
2. First name, last name.
3. First name, middle initial, last name.

In June we received a refund check from the state taxation department, with the same erroneous form of my name. I was prepared to put up with it for a driver's license, but taxation is another story altogether. I wrote a letter to the department at the time, and today I heard back from them.

It seems that the taxation department has moved to the same computer system. The person I spoke with said that the old system was removed and the new one brought into production December 15 of last year, with no overlap period and no preliminary real-life testing, and they have been reporting problems with it ever since (surprise!). This is just one more. She is passing it on to the section head to bring up at the weekly meeting with the systems people. Given that this package is used in more departments than theirs, though, a change will probably not be trivial.

In addition to rejecting all but the forms shown above, the

system does not accept embedded blanks (e.g. "Mary Ann"), periods, or even hyphens (!) in names. Worse, it cannot take both given names in full - i.e. the legal name that appears on one's birth certificate, passport, SS card, etc. (Although I didn't ask, I strongly suspect that it will not accept multiple middle initials, either.)

This strikes me as more than just an issue of people being forced to fit within unnecessary software limitations. By restricting the forms of names, they increase the chance of namespace collisions (especially on driver's licenses, where the name is often the only common key across states). Since the IRS doesn't appear to have this problem, there will be mismatches in the combination of SSN+name in the state and federal tax records. This could potentially make it harder to identify phony SSN numbers and bad duplicates. And it will add to the opinion held by many people that "computers" are dictating their lives, when in fact it's the people specifying and designing the software who are doing that.

If anyone has any more information about this database project, I would be very interested in hearing it.

M. Ruth Milner, Assistant to the Director -- Computing, NRAO,
Socorro NM
rmilner@nrao.edu 1-505-835-7282 FAX 505-835-7027

[This is an OLD tale in RISKS, but worth repeating, because it does not seem to go away. PGN]

🔥 REVIEW: "Personal Encryption Clearly Explained", Pete Loshin

Rob Slade <rslade@sprint.ca>

Wed, 21 Oct 1998 09:55:17 -0800

BKPERENC.RVW 980726

"Personal Encryption Clearly Explained", Pete Loshin, 1998,
0-12-455837-2, U\$39.95/C\$55.95

%A Pete Loshin pete@loshin.com

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

%D 1998

%G 0-12-455837-2

%I Academic Press/Academic Press Professional/Harcourt Brace

%O U\$39.95/C\$55.95 800-321-5068 fax: 619-699-6380 app@acad.com

%P 545 p.

%T "Personal Encryption Clearly Explained"

I am getting just a little tired of the car analogy.

"You don't need to be a mechanic," so the metaphor goes, "to drive a car.

Therefore, you don't need to know anything about the theory behind

[encryption|networking|programming|etc.] in order to use a computer." This

comparison ignores two important points. One is that in 1912 you *did* need

to be a fair mechanic to operate a car effectively, and that is roughly

where we are with regard to the development of the computer.

The second

point is that while computer programs are generally easy enough for a novice

to use once they have been set up, the choice, evaluation, and configuration

of systems requires much more background. Particularly in the field of

encryption, in recent times "experts" have been recommending systems for

which the time needed to crack keys has fallen to literally hours.

This book purports to give you everything that you need in order to both use and understand encryption, specifically with regard to digital signatures.

While the text does provide some limited conceptual education and a little vicarious experience with a handful of commercial products it cannot be said to deliver on its promise.

Chapter one is a bit hard to define. It seems to start out as a sales pitch, trying to convince the reader that encryption is important. However, it also looks at the scope of privacy and threats thereto, and even starts to develop the background for encryption technologies. The quality is highly uneven. A discussion of security versus usability is excellent and notes that the convenience of modern personal networking systems pose tremendous security vulnerabilities. On the other hand, the introduction to information risks cites only computer criminals, without considering the possibility of transmission of sensitive information to unauthorized recipients through human errors or system failures. A review of types of data that should be secured fails to note that encrypting some files and messages while leaving others accessible can, in and of itself, provide assistance to the enemy. The material on security technologies and specific threats is fairly mundane.

A primer on encryption is presented in chapter two, although it is, as is all to usual, more of a history than a real explanation. Modern computer

encryption is less than half of the chapter, and most of that space is dedicated to describing different applications rather than technologies.

Appendix A should probably be considered as an extension of the discussion,

and does provide a first rate explanation of the mathematical underpinnings

to modern public-key encryption, but ends just as we get to the good bit.

Neither the chapter nor the appendix gives the necessary preparation for

assessing cryptographic strength.

Chapter three is a balanced but relatively superficial examination of the

debate surrounding the US government's attempts to restrict the availability

and use of encryption. The discussion of encryption implementation in

chapter four touches on a wide range of issues, but none in any depth. A

number of disparate products are briefly described (and the "installation"

of two is presented in some detail), but the foundation for evaluation still

has not been provided in chapter five. Chapter six looks at a number of

security topics and features related to the Netscape Navigator browser, but

not all relate to encryption, and encryption related topics are passed over

quite quickly. There is, for example, no discussion of the ramifications of

dealing with either "export" copies of Netscape products, or non-US Web

servers, both of which may be restricted in the cryptographic keys they can

deal with. Operational, but not functional, specifics of three e-mail

products with cryptographic capabilities are detailed in chapter seven.

Similar information is given for some file encryption products

in chapter
eight.

Chapter nine's explanation of digital commerce is simplistic and surprisingly abrupt. The review of key management in the Network Associates PGP product should be viewed together with the material in chapters five and eight (and even then isn't really complete) but additional content does begin to address some of the conceptual issues in chapter ten.

This is yet another example of a book that tries to explain encryption to a non-technical audience but seems to feel that a full background is not needed. Loshin does a better job than some other authors with the inclusion of Appendix A, but fails to provide either the explanation of function or the demonstration of relative strength that Garfinkel manifested in "PGP: Pretty Good Privacy" (cf. BKPGPGAR.RVW). Unfortunately this current work is neither clear not complete enough to be recommended for any particular audience.

copyright Robert M. Slade, 1998 BKPERENC.RVW 980726

⚡ Dependable Computing for Critical Applications: CFP

Chuck Weinstock <weinstock@sei.cmu.edu>
Tue, 20 Oct 1998 11:51:49 -0400

CALL FOR PARTICIPATION
Seventh IFIP International Working Conference on
Dependable Computing for Critical Applications (DCCA-7)
The Fairmont Hotel
San Jose, California, USA

January 6-8, 1999

[See <<http://www.conjelco.com/dcca/>> for the full Call for Participation.

This item is abridged for RISKS. PGN]

This is the seventh conference in a series dedicated to advancing the theory and practice of dependable computing for critical applications. DCCA differs from other conferences on related topics in encouraging participation across all fields that contribute to dependable computing, and in its format as a working conference that provides ample time for discussion; these attributes provide for a stimulating meeting that facilitates cross-fertilization of ideas and interaction between researchers and practitioners.

General Chair: Charles B. Weinstock, Software Engineering Institute, USA

Program Chair: John Rushby, SRI International, USA

PRELIMINARY CONFERENCE SCHEDULE (tentative)

Wednesday January 6, 1999

9 am: Assessment of COTS Components

There is increasing pressure to use COTS (commercial off-the-shelf)

components in critical systems. How dependable are these components? These

two papers respectively examine design faults in a commercial processor

(Pentium II), and the reliability of a commercial microkernel

(Chorus

ClassiX).

* The Taxonomy of Design Faults in COTS Microprocessors by Algirdas

Avizienis and Yutao He of UCLA, USA

* Assessment of COTS Microkernels by Fault Injection by J.-C. Fabre, F.

Salles, M. Rodriguez-Moreno, and J. Arlat of LAAS, France

11am: Coping with COTS

These two papers respectively describe how to construct a reliable spacecraft controller and fault-tolerant clocks from COTS components.

* Minimalist Recovery Techniques for Single Event Effects in Spaceborne

Microcontrollers by Douglas W. Caldwell and David A. Rennels of UCLA, USA

* Building Fault-Tolerant Hardware Clocks from COTS Components by

Christof Fetzner and Flaviu Cristian of UCSD, USA

2pm: Formal Methods

Formal methods can help develop verified systems, and can also be used to examine requirements and designs for bugs. The first of these papers uses theorem proving to develop verified controllers, while the other two use model checking in the validation of complex requirements.

* A methodology for proving control systems with Lustre and PVS by S.

Bensalem, P. Caspi, C. Parent-Vigouroux, and C. Dumas, D. Pilaud,

VERIMAG, France

* Prototyping and Formal Requirement Validation of GPRS: A Mobile Data

Packet Radio Service for GSM by Luigi Logrippo, Laurent Andriantsiferana, and Brahim Ghribi of University of Ottawa, Canada

* Formal Description and Validation for an Integrity Policy Supporting

Multiple Levels of Criticality by A. Fantechi, S. Gnesi, and L. Semini

of University di Firenze, Italy

4:30pm: Distributed Systems

The first of these papers develops an infrastructure for fault-tolerance on top of CORBA; the second considers how to improve performance of one of the protocols used in such infrastructures.

- * Proteus: A Flexible Infrastructure to Implement Adaptive Fault Tolerance in AQUA by Chetan Sabnis, Michel Cukier, Jennifer Ren, William H. Sanders, David E. Bakken, and David Karr of University of Illinois and BBN, USA
- * Improving Performance of Atomic Broadcast Protocols Using the Newsmonger Technique by Shivakant Mishra and Sudha M. Kuntur of University of Wyoming, USA

Thursday January 7, 1999

9am: Time-Triggered Architecture

The time-triggered architecture (TTA) provides a robust foundation for critical control applications such as drive-by-wire. The first paper describes how fault-tolerant applications can be supported in this architecture, while the second describes formal verification of the clock-synchronization protocol used in TTA.

- * The Transparent Implementation of Fault Tolerance in the Time-Triggered Architecture by Hermann Kopetz and Dietmar Millinger of TU Vienna, Austria
- * Formal Verification for Time-Triggered Clock Synchronization by Holger Pfeifer, Detlef Schwier, and Friedrich W. von Henke of University of Ulm, Germany

11am: Fault Tolerance and Safety

The redundancy added to provide fault tolerance can introduce new failure modes that may compromise safety. The first paper describes such a situation and presents a protocol that overcomes it. The second paper describes validation of fault tolerant systems by fault injection.

* PADRE: A Protocol For Asymmetric Duplex Redundancy by Didier Essame,

Jean Arlat, and David Powell of LAAS, France

* Experimental Validation of High-Speed Fault-Tolerant Systems Using

Physical Fault Injection by R. J. Martìnez, P. J. Gil, G. Martìn, C.

PÈrez, and J.J. Serrano of the University and Politecnica of Valencia, Spain

2pm: Models of Partitioning for Integrated Modular Avionics

Integrated Modular Avionics (IMA) bring together several airplane control

functions that were previously performed by separate computer systems. This creates new opportunities for fault propagation that must be eliminated by partitioning. But what exactly are the requirements for safe partitioning?

These three papers attempt to answer this question using models that have their roots in computer security.

* A Model of Cooperative Noninterference for Integrated Modular Avionics

by Ben L. Di Vito of ViGYAN/NASA Langley, USA

* Invariant Performance: A Statement of Task Isolation Useful for

Embedded Application Integration by Matthew M. Wilding, David S.

Hardin, and David A. Greve of Collins Commercial Avionics,

USA

* A Model of Non-Interference for Integrating Mixed-Criticality Software

Components by Bruno Dutertre and Victoria Stavridou of SRI International, USA

Dependability Evaluation

For some, dependability is closely related to reliability; for others, it

is a more complex mix of properties. The first paper applies classical

reliability modeling to phased missions, while the second proposes a method

for evaluating a system against multiple criteria.

* Dependability Modeling and Evaluation of Phased Mission Systems: a

DSPN Approach by Ivan Mura, Andrea Bondavalli, Xinyu Zang, and Kishor

Trivedi of University of Pisa and CNUCE/CNR, Italy, and Duke University, USA

* Dependability Evaluation using a Multi-Criteria Decision Analysis

Procedure by Divya Prasad and John McDermid of the University of York,

UK

Friday January 7, 1999

9am: Panel: Certification and Assessment of Critical Systems

It is difficult or impossible to measure some important attributes of

critical systems (e.g., experimental quantification of failure rates in the

10⁻⁹ range is infeasible). Therefore, many of the standards for critical

software development (e.g., DO-178B, IEC1508, the Common Security Criteria)

focus on the development process: "we cannot measure how well you did, so

we measure how hard you tried." Some criticise these standards for having

requirements whose compliance cannot be objectively determined,

or for
requiring use of techniques whose efficacy has not been
established. Others
note that multiple sources of evidence are required in assessing
a critical
systems, and ask how best to combine these different sources.

This panel will comprise experts representing a range of opinion
who will
examine the topic of certification and assessment of critical
systems from
several perspectives.

11:30am: Probabilistic Guarantees

The first paper considers scheduling in the presence of faults,
while the
second considers detection of faulty components. Both papers
employ
statistical methods.

* Probabilistic Scheduling Guarantees for Fault-Tolerant Real-
Time

Systems by A. Burns, S. Punnekkat, L. Strigini and D. R.
Wright of the
University of York and City University, UK

* Fault Detection for Byzantine Quorum Systems by Evelyn
Pierce, Lorenzo

Alvisi, Dahlia Malkhi, and Michael Reiter of University of
Texas at
Austin, and Bell Laboratories, USA

1 pm Adjourn



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 5

Friday 6 November 1998

Contents

- [Labor has premature delivery](#)
[R Romine](#)
- [ABC News posts election results before the election!](#)
[Martin Minow](#)
- [Salt Lake ATC center radar blackout affects 200 planes](#)
[Richard Schroepel](#)
- [AT&T Loses over 400 T3s](#)
[Sean Sosik-Hamor](#)
- [NYSE stock market crash -- well, the other kind!](#)
[Declan McCullagh](#)
- [Microsoft execs worry about free software movement](#)
[Edupage](#)
- [Microsoft and the Halloween Documents](#)
[PGN](#)
- [Computer keeps 100 pounds per week from pensioners](#)
[Peter Leeson](#)
- [Stores' shoplifting gates can set off pacemakers, defibrillator](#)
[Keith Rhodes](#)
- [Swedish train-ticket reservation system down](#)
[Ulf Lindqvist](#)

- [SAS airline timetables: Internet 1, Hardcopy 0](#)
[Martin Minow](#)
 - [New Swedish law makes most of the Internet illegal](#)
[Jacob Palme](#)
 - [Stanford e-mail system passwords stolen](#)
[Monty Solomon](#)
 - [Rats take a byte out of Ugandan exam computers](#)
[ejm](#)
 - [Grave error!](#)
[Dave Stringer-Calvert](#)
 - [Re: SRI voice-mail woes](#)
[Peter Kaiser](#)
 - [Re: Another wild bank saga](#)
[PGN](#)
 - [Jon Postel](#)
[PGN](#)
 - [REVIEW: "Democracy and Technology", Richard E. Sclove](#)
[Rob Slade](#)
 - [REVIEW: "Windows NT Server 4 Security Handbook", Hadfield/Hatter/Bixler](#)
[Rob Slade](#)
 - [Promoting Formal Methods](#)
[Dilia E. Rodriguez](#)
 - [FMICS4 1st CFP](#)
[Diego Latella](#)
 - [SAFECOMP 99 - CFP](#)
[Pasquini](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Labor has premature delivery

<rromine@nsf.gov>

Fri, 06 Nov 98 09:47:59 EST

Everyone on Wall Street and elsewhere eagerly awaits the official Bureau of Labor Statistics statistics, which were due to be posted on

their Web site today. The BLS takes great pains to avoid leaks. However, much to everyone's surprise, some tables appeared YESTERDAY. As a consequence, BLS Commissioner Katharine G. Abraham decided to release the full report yesterday afternoon. The interpretations were favorable, and the stock market had a big gain. Abraham was quoted as saying that even if the early release ``was a computer error, it was a human failure'' in that the system was not set up to prevent it.

A prior early release occurred in January 1997, when the Federal Reserve's Beige Book was released at noon instead of 2 p.m., because no one bothered to tell the Web site administrators that the time had been delayed.

[Source: Web Goof Leaks Data, Moves Stocks, By John M. Berry
The Washington Post, 6 Nov 1998, Page F01; PGN Stark Abstracting]

⚡ ABC News posts election results before the election!

Martin Minow <minow@apple.com>
Wed, 4 Nov 1998 10:15:24 -0800

According to the Drudge Report <<http://www.drudgereport.com>>, ABC News posted ``final election results'' on its web site late Monday night, i.e., before the election began. According to an apology from ABC News (also quoted by Drudge) -- and reading between the lines -- they apparently posted test data on their live Internet server. ABC News's web site is

<<http://www.abcnews.com>>. My very brief look at the ABC News site did not turn up any explanation or apology on their site.

Martin Minow, minow@pobox.com

[For example, the dummy data showed incumbent Sen. Alfonse D'Amato (Rep.) besting Charles E. Schumer (Dem) in the New York Senate race, which turned out to be wrong. PGN]
[Declan McCullagh <declan@well.com> noted an article by Adam Clayton Powell III on the same story, noting that ABC had the right outcome on 61 out of 70 Senate and Governor races. That article also noted that Fox TV had accidentally put up an advance dummy page for a Yankee-Padre World Series game -- and almost got it correct! PGN]

⚡ Salt Lake ATC center radar blackout affects 200 planes

Richard Schroepel <rcs@VISI.NET>
Thu, 5 Nov 1998 12:03:50 -0500 (EST)

On 4 Nov 1998, the primary and backup radar systems for the Salt Lake Air Traffic Control Center failed for about a minute, leaving about 200 planes ``up in the air'' over Utah, Nevada, Idaho, Montana, and Wyoming. Handoffs were done manually (actually, orally). [Source: 4 Nov 1998, <http://www.nandotimes.com>]

⚡ AT&T Loses over 400 T3s

Sean_Sosik-Hamor <hamors@aloft.micro.lucent.com>

Wed, 28 Oct 1998 12:50:40 -0500

We're not sure when the fault (probably a fiber cut, but that's unconfirmed) actually happened, but Lucent Microelectronics in Allentown, PA lost all network connectivity at approximately noon today. AT&T lost approximately 400 T3s, which caused every single Lucent router nationwide to try to relearn their routes and effectively pegged all routers at 100%.

Because of this, a second outage occurred due to the fact that the routers were too busy relearning their routes to actually pass traffic. This was a nationwide outage for both Lucent and AT&T. As of 01.45pm, Lucent locations in Allentown, PA have isolated all traffic from the backbone, so at least we're back up and running.

Sean

⚡ NYSE stock market crash -- well, the other kind!

Declan McCullagh <declan@well.com>

Mon, 26 Oct 1998 16:00:19 -0500

Trading on the New York Stock Exchange was halted at 1:16 p.m. for just under an hour on 26 Oct 1998, because of "equipment problems". [<http://www.wired.com/news/news/business/story/15837.html>]

⚡ Microsoft execs worry about free software movement

Edupage Editors <educause@educause.unc.edu>

An internal Microsoft memo written by one of that company's software engineers indicates that Microsoft is concerned with developing strategies for competing against free programs that have been gaining popularity with software developers, such as the operating system Linux. The memorandum warns that the usual Microsoft marketing strategy known as FUD (an acronym for fear, uncertainty, and doubt) won't work against developers of free software, who are part of the OSS (open-source software) movement that makes source code readily available to anyone for improvement and testing. The memo (<http://www.opensource.org/halloween.html>) says: "The ability of the OSS process to collect and harness the collective I.Q. of thousands of individuals across the Internet is simply amazing. More importantly, OSS evangelization scales with the size of the Internet much faster than our own evangelization efforts appear to scale." (*The New York Times*, 3 Nov 1998; Edupage, 3 Nov 1998)

⚡ Microsoft and the Halloween Documents

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

Fri, 6 Nov 98 8:47:21 PST

A second of the so-called Halloween Documents, written by Microsoft people

and lightly annotated by Eric Raymond (the first so-called because it was analyzed by Eric over the Halloween weekend), is also available. Analyzing the perceived threats to Microsoft represented by open-source software, the documents are also fascinating testaments to the appeals of open-source software. The first

<http://www.opensource.org/halloween.html>

was noted above, with Eric's alternative source as

<http://www.tuxedo.org/~esr/halloween.html>

The second is at

<http://www.opensource.org/halloween2.html>

🔥 Computer keeps 100 pounds per week from pensioners

"Peter Leeson" <Peter@gpysl.globalnet.co.uk>

Thu, 5 Nov 1998 06:30:55 -0000

Approximately 200,000 elderly Brits are not receiving their proper state pensions because of a computer glitch, losing up to 100 pounds a week for the past few months. The problem is blamed on the cutover to a new 170-million-pound computer system, and according to a government source is likely to take another five months to fix. [Source: Jon Hibbs, *London Daily Telegraph*, 5 Nov 1998; PGN Abstracting]

🔥 Stores' shoplifting gates can set off pacemakers, defibrillator

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

Thu, 05 Nov 1998 12:46:51 -0500

Today's *New England Journal of Medicine* notes a case of a 72-year-old man whose defibrillator was affected by interference from a Sensormatic Ultra-Max anti-theft device in a bookstore's shoplifting gate. Fortunately, a nurse caught him, recognized the source of the problem, and pulled him away. The head of The Heart Institute of St. Petersburg, Florida, noted that this is the most popular device -- with 91,000 in use.

Debbie Coller of Sensormatic noted that the FDA advisory panel had found no significant health hazard. "Shoplifting gates have been around for about 25 years," she said. "Heart pacemakers have been around even longer. During that time, 1 billion safe passages already have occurred." [Source: Associated Press item, 4 Nov 1998; PGN Abstracting]

[But RISKS readers may recall that heart-pacemaker interference deaths were reported in 1980 and 1985, and defibrillator interference was discussed in [RISKS-19.50.52.53](#). This not a new problem. PGN]

[An error in the original has been corrected in the archive copy. PGN]

🔥 Swedish train-ticket reservation system down

Ulf Lindqvist <ulfl@ce.chalmers.se>
Thu, 29 Oct 1998 14:45:44 +0100 (MET)

Here is yet another example of a backup system that does not work when

needed. [Source *Goteborgs-Posten*, via Tidningarnas
Telegrambyra News
Service, 29 Oct 1998; Ulf Lindqvist abstracting and translating.]

The central computer for ticket sales and reservations at the
Swedish
railway company (SJ) was down during the entire day, Wednesday
28 Oct 1998.
Phone ticket sales, normally serving 15,000 customers every day,
were
completely shut down and at local sales offices only fare
tickets without
reservations could be purchased. The company press information
officer
explains: ``There was a hardware failure in the mainframe
supporting our
entire system. This also caused the backup computer to fail.''

Ulf Lindqvist, Computer Engineering, Chalmers University of
Technology
SE-412 96 Goteborg, SWEDEN +46 31 772 1760 ulfl@ce.chalmers.
se

✶ SAS airline timetables: Internet 1, Hardcopy 0

Martin Minow <minow@apple.com>
Thu, 29 Oct 1998 15:12:14 -0800

Here's a new variant on a data error: according to a press
report, the
printed edition of Scandinavian Airlines (SAS) winter timetable
is
completely wrong -- the printers mistakenly reprinted 350,000
copies of the
summer timetable.

Fortunately, the timetable available on the Internet and over
the telephone
is correct.

Martin Minow <minow@pobox.com>

[Also noted by Debora Weber-Wulff <Debora.Weber_Wulff@te.mah.se>, who is in Sweden on sabbatical. PGN]

🔥 New Swedish law makes most of the Internet illegal

Jacob Palme <jpalme@dsv.su.se>
Sun, 25 Oct 1998 08:51:12 +0200

[Thanks to Dan Wing of Cisco for forwarding. PGN]

A new Swedish law which makes most of the Internet illegal in Sweden took effect yesterday. The law is named personal information handling law. It makes much of the publication of information about individual persons on the Internet illegal, such as criticism of named persons, publication of lists of references in scientific papers or the sending of e-mail messages outside of Europe.

More about the new law at URL

<http://www.dsv.su.se/~jpalme/society/personal-register-law.html>

(note: The Swedish government will probably not use the law to stop Internet. This law and other laws like it have made me understand that laws are not meant to be obeyed.)

Question: All other EU countries are to enact similar laws. Have other countries interpreted the EU directive in the same way, and developed laws

which would make most of the Internet illegal?

Jacob Palme <jpalme@dsv.su.se> (Stockholm University and KTH)
for more info see URL: <http://www.dsv.su.se/~jpalme>

✶ Stanford e-mail system passwords stolen

Monty Solomon <monty@roscom.com>

Wed, 4 Nov 1998 03:42:42 -0500

Beginning about three weeks ago, about 4,500 Stanford e-mail users had their passwords captured by a sniffer, planted because not all systems had been properly upgraded with new security features. The sniffer was detected only a few days ago. The attack was apparently carried out from Sweden and Canada. [Source: Reuters item, 3 Nov 1998, special to CNET, <http://www.news.com/News/Item/0,4,28303,00.html>; PGN Abstracting]

✶ Rats take a byte out of Ugandan exam computers

<e_j_m@yahoo.com>

Tue, 13 Oct 1998 21:09:52 GMT

The computer system used to determine thousands of university places (based on national exams) crashed because of rats having chewed through cables. Rats had previously severed phone links to parts of western Uganda and Rwanda. [Source: Reuters item, <http://www.cnn.com/WORLD/africa/9810/13/RB000657.reut.html> PGN Abstracting]

Just goes to show that hackers come in all shapes and sizes. :) [ejm]

[The rats were snackers rather than hackers, but they prevented the examiners from separating the knackers from the slackers. PGN]

⚡ Grave error!

Dave Stringer-Calvert <dave_sc@csl.sri.com>
Fri, 30 Oct 1998 15:04:37 -0800

The risks of Automated Mailing Software....

Embarrassed council officials have apologised for asking the occupant of a village cemetery to fill in a survey. A questionnaire from Rushcliffe Borough Council asked 'The Occupier, Burial Ground' in Flintham, Notts, if he or she had been a victim of crime in the last 12 months or belonged to a Neighbourhood Watch Scheme. The wrongly-addressed letter was among 2,000 sent out to businesses in the area as part of a survey to pinpoint concerns over crime and vandalism. But a council spokesman admitted: 'There is not much chance of a reply being received from the occupant there.' [...]
[From Yorkshire Evening Press, 10/30/98]

⚡ Re: SRI voice-mail woes (PGN, [RISKS-20.04](#))

Peter Kaiser <kaiser@acm.org>

Thu, 22 Oct 1998 08:38:49 +0200

> The absence of both voice-mail and call-forwarding
> certainly makes life tough.

But simpler, I should think -- it certainly does in my life.
Indeed, on an occasion when several hundred persons (including me) lost computer service at our desktops at work for ten days, work life in our building became extremely simple, if at a rather higher emotional voltage.

At home we used to have an answering machine, but my wife -- more or less a technophobe -- hated it, so I disconnected it. Since then I tell people that our not having an answering machine is a service to our callers, subtly signalling them that we either are away or don't wish to answer the phone, thereby saving them the connection charges.

Pete kaiser@acm.org, pekaiser@access.ch

✶ Re: Another wild bank saga ([RISKS-20.04](#))

"Peter G. Neumann" <Neumann@CSL.sri.com>

Tue, 27 Oct 1998 13:12:09 -0400

Yes (as noted by many readers), I was unable to disremember some of the earlier confusion between the British BILLION and the American BILLION. In the olden dayes in England (until a few decades ago), the Brits commonly used the European MILLIARD which is equivalent to the American BILLION, with their BILLION equivalent to the American TRILLION. Apparently

the Brits
have informally switched in common usage, although the French
and Germans
still use the MILLIARD. The confusion is commonly resolved by
referring to
a thousand million or a million million. Perhaps the Euro
presents an
opportunity to standardize, but I have not heard any such news.

Jon Postel

"Peter G. Neumann" <Neumann@CSL.sri.com>

Tue, 20 Oct 1998 07:55:17 -0400

Jon Postel was one of the real pioneers of the ARPAnet/Internet,
first at
SRI (then Stanford Research Institute) and then at ISI.
Recently, he was
head of the IANA (Internet Assigned Numbers Authority).
Although there are
still many network risks remaining, Jon was instrumental in many
different
ways in making the existing networks as operationally robust as
they have
become. He will be deeply missed.

REVIEW: "Democracy and Technology", Richard E. Sclove

"Rob Slade" <rslade@sprint.ca>

Fri, 30 Oct 1998 09:58:02 -0800

BKDEMTEC.RVW 980816

"Democracy and Technology", Richard E. Sclove, 1995, 0-89862-861-
X,
U\$18.95

%A Richard E. Sclove
%C 72 Spring Street, New York, NY 10012
%D 1995
%G 0-89862-861-X
%I The Guilford Press
%O U\$18.95 212-431-9800 fax: 212-966-6708 staff@guilford.com
%P 319 p.
%T "Democracy and Technology"

"This book promotes the reconstruction of technology along more democratic lines. [...] Insofar as (1) citizens ought to be empowered to participate in shaping their society's basic circumstances and (2) technologies profoundly affect and partly constitute those circumstances, it follows that (3) technological design and practice should be democratized." Personally, I can sympathize with the aims, and even the thesis, that the author proposes for this text. However, he also notes a personal experience that taught him "that even the most well-intentioned, elite study group can be deeply unaware of the extent to which its conclusions embody far-reaching value judgements." What Sclove seems to have missed is the fact that however important your ideas may be, they have to be communicated to those who may have different backgrounds, and also have to be backed up by some kind of evidence. Although the declamations may be impassioned, only the most sympathetic and dedicated reader will be able to plow through the prose; and the arguments, as they proceed, have little support beyond force of personality.

Part one is intended to synthesize modern research in the social dimensions

of technology and democratic theory into a rudimentary but comprehensive democratic theory of technology. Chapter one, using a statistical sampling of two communities (one of which is oversimplified into caricature) states that technology affects society, but that society can choose those technologies that it will accept. The idea that technology affects society is re-examined in greater detail and verbiage in chapter two. Democratic decision-making is said to be superior in chapter three, and some objections are replied to. Unfortunately, this entire section is based on only four real examples, and those situations include one failure, one closed and homogeneous community, and two "megaprojects" requiring massive, formal bureaucratic and political decisions. The theory eventually turned out is extremely rudimentary: it states that technology should be democratized, but fails to determine whether it can be.

Part two proposes a set of evaluation points that can be used to review technologies for compatibility with democracy. Chapter four is supposed to look at technologies of community, but concentrates primarily on work situations. In this regard it weakens the arguments of part one in that examples are given of cooperative social structures (successfully) imposed on hierarchical work environments, and democratically designed work technologies subsumed to a centralized corporate structure. When the topic does finally turn to a purer consideration of community it is to dismissively denigrate the possibility of technological support of virtual

community. Democratic work is said to be free of routine and inflexible schedules, but chapter five singularly fails to say how this utopian state of affairs is to be accomplished. The first of three discussions of politics, chapter six proposes that technologies that promote distorted ideologies or exacerbate social inequities be avoided. Actually, though, the material hardly touches on any example technologies at all. Two of the points in chapter seven boil down to "smaller is prettier" since technologies with a smaller scope of impact promote local self-governance. The third, however, is rather vague. We are to prefer technologies that promote decentralization and federation, without any real ideas of what those are. (There is also no analysis of the relative importance of self-governance versus federation, a debate that my Canadian heritage finds most compelling.) The first point in chapter eight is that we should not foul our own nests, and I assume that most would agree with that; the only problem being the determination of how strictly to adhere to it. The second, however, seems to be an almost religious insistence on flexibility. For the perpetuation of a species we might note that adaptability is a good thing, but technology can be managed by the species (that is, us) according to changing conditions. Is the slotted screw somehow morally superior to the Robertson because slotted screwdrivers can be used as (rather clumsy) chisels?

Part three is a defence of the democratic politics of technology against

traditional economic models. Chapter nine appears to want to eliminate the concept of value from the discussion. Economic theory is not actually challenged in chapter ten. Instead it is turned into a straw-philosophy, "economism," and attacked as unfit for comparison with social justice. I fully agree with the kind of participatory inventiveness that chapter eleven espouses, which used to go by the name of amateur scholarship. It cannot, however, be successfully mandated: it must be self-driven. This has to be obvious from the examples given in the chapter which are almost universally either proper systems analysis stories or failures. Chapter twelve purports to lay out a roadmap for pursuing more democratic technologies, but is weakened by a vast majority of statements that use "could" or "might" rather than "will." Sclove does admit to a number of important social factors that work against his ideals (at least in the United States) in chapter thirteen, but finishes by only hoping that they can be overcome.

This book is forceful, turgid, passionate, dull, and verbose. At first reading, I thought that the nine criteria for evaluation of technologies were the most important part of the work. However, as an exercise I tried reviewing some processes. War and weapons technologies came out surprisingly well, marred only by a tendency to perpetuate authoritarian structures. Guerilla or sectarian violence came out even better. Again, I am in full agreement with the general aims of the book, but have to conclude that a lot more work needs to be done on the specifics.

copyright Robert M. Slade, 1998 BKDEMTEC.RVW 980816

✦ REVIEW: "Windows NT Server 4 Security Handbook", Hadfield/Hatter/Bixler

"Rob Slade" <rslade@sprint.ca>
Mon, 2 Nov 1998 11:45:58 -0800

BKNT4SHB.RVW 980814

"Windows NT Server 4 Security Handbook", Lee Hadfield/Dave
Hatter/Dave

Bixler, 1997, 0-7897-1213-X, U\$39.99/C\$56.95/UK#36.99

%A Lee Hadfield

%A Dave Hatter dhatther@definiti.com

%A Dave Bixler dbixler@art-deco.net

%C 201 W. 103rd Street, Indianapolis, IN 46290

%D 1997

%G 0-7897-1213-X

%I Macmillan Computer Publishing (MCP)

%O U\$39.99/C\$56.95/UK#36.99 800-858-7674 info@mcp.com

%P 476 p.

%T "Windows NT Server 4 Security Handbook"

Part one is an overview, both of security and Windows NT. Chapter one's presentation of security basics has many good points, but also some unfortunate gaps and errors. The review of security concepts in NT provides a good grounding in how the matter is seen from Microsoft's perspective in chapter two. (It also has a rather interesting quick introduction to firewalls.) The NT architecture overview in chapter three does not really concentrate on security topics. When it does, the coverage of access control is reasonably clear, if not terribly readable.

The Implementation of security, in part two, explains individual functions well but does not provide conceptual frameworks for security operations. Most of the material does provide the ideas behind a feature, but then simply follows through the screens for turning it on. Topics include domains, trust relationships, NTFS (New Technology File System) security, protecting domain resources, and NT Workstation security. Somewhat different is chapter six, which gives a thorough tutorial on internal user authentication procedures.

Part three walks through the implementation of a master domain network. Chapters cover planning, implementation steps, and configuration of trust relationships, but the material is too brief for a realistic guide. Part four looks at security for various related products, such as BackOffice, NetWare, Macintosh, Internet, and UNIX. Again, there are more mentions than working details. Part five first explains and then walks you through implementation for C-2 security configuration.

Of those I have reviewed to date, this book delves deepest into many areas of NT security and protection. However, it still does not draw back the shroud surrounding the NT security model. The explanations of operations are clear and there is much useful information, but still no clear direction to the besieged sysadmin.

copyright Robert M. Slade, 1998 BKNT4SHB.RVW 980814

✦ Promoting Formal Methods

"Dilia E. Rodriguez" <rodrigue@AI.RL.AF.MIL>

Thu, 22 Oct 1998 08:15:33 -0400 (EDT)

Coming of Age Formal Aspects of Computing at 21
2nd December 1998, British Royal Society

The 21st anniversary of the British Computer Society Formal
Aspects of Computing Science Special Interest Group

To mark this coming of age, we have invited four of our
distinguished
Fellows of the British Royal Society to select highlights of
current
research achievements, reflect on past lessons learned and look
forward to
future directions.

Mike Gordon 21 Years of Hardware Verification

Tony Hoare Top-down and bottom-up and meeting in the
middle

Robin Milner Computing is Interaction

Gordon Plotkin On Syntax

This 21-year period has seen formal methods mature from
inception as a
purely academic research area, to establish itself in computer
science
curricula, and most recently to be practically applied in
industry.

The FACS at 21 meeting will take place at The Royal Society, 6
Carlton House
Terrace, London, commencing 9.30 am and finishing by 5.00 pm. In
addition,
there will be an opportunity to attend an evening meal attended
by the
speakers. (Registration form below.)

For more information contact: Computing Research Centre, School
Of Computing
and Management Sciences, Sheffield Hallam University, Sheffield,
S1 1WB, UK.
Tel. +44 (0) 114 225 5555. Current information is available at:

<http://www.shu.ac.uk/facs21>

FMICS4 1st CFP

Diego Latella <d.latella@cnuce.cnr.it>
Wed, 28 Oct 1998 11:29:56 +0100 (MET)

ERCIM Working Group on Formal Methods for Industrial Critical
Systems

Fourth International Workshop
Formal Methods for Industrial Critical Systems
(PRELIMINARY CFP)
July 11-12 1999

[http://www.cnuce.pi.cnr.it/cnuweb/research/resgroups/conc-meth/
FMICS/WS/Trento99/workshop.html](http://www.cnuce.pi.cnr.it/cnuweb/research/resgroups/conc-meth/FMICS/WS/Trento99/workshop.html)

Deadline for submission: March 1st, 1999, to
S. Gnesi, CNR-IEI, Via S. Maria 46, I56126 Pisa - ITALY
telephone: +39 050 593489

SAFECOMP 99 - CFP

<pasquini@infos1.casaccia.enea.it>
Mon, 02 Nov 1998 17:22:22 +0100

Safety, Reliability and Security of Computer Systems
Toulouse, France, 27-29 September 1999

Submissions by 31 Jan 1999.

<http://www.laas.fr/safecomp>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 6

Thursday 12 November 1998

Contents

● [Risk Management is Where the Money Is](#)

[Dan Geer](#)

⚡ Risk Management is Where the Money Is

Dan Geer <geer@certco.com>

Wed, 11 Nov 1998 22:20:09 -0500

Digital Commerce Society of Boston

3 November 1998

Daniel E. Geer, Jr., Sc.D.

Senior Strategist, CertCo, Inc.

55 Broad Street, NYC, and

100 Cambridgepark Drive, Cambridge

geer@certco.com

Given my biases, I am going to describe where the future of the security marketplace is and where it is not. I will argue that the financial

community is and remains the place to look for "first light" for new security technology. I will give you a rundown of what's new while I predict what little time is left for many of today's products, purveyors and regulators. I will argue that, in many ways, the party's over for the security field as we know it now. I will range broadly because security, as a concept, is universal.

"Nothing is so powerful as an idea whose time has come." For security technology, that time is now. IBM calls the three requirements of the "e-business" future as: #1 security, #2 scalability, and #3 integration. Forrester, Gartner, META, Yankee and all the other analysts agree -- the most important enabling technology for electronic business, besides network connectivity itself, is security. AD Little estimates that security, privacy and the legal issues of digital signature together constitute over half of the quantifiable barriers to electronic commerce. There are whole venture funds whose investment focus is around security. Security startups are everywhere; so are security books. The word "security" is hardly rare in employment advertisements. You cannot walk a trade show and not see the word "security" in screaming big type. The number of security meetings is preposterous. Presidential Commissions are busy spending real money on security for the information systems that run the country.

"In the future, everyone will each get 15 minutes of fame." That applies to security, too. Today's security specialty companies cannot

all survive; they can be eclipsed by the platform vendors too easily.

Only platform vendors can deliver security that is integrated enough to scale and invisible enough to ignore. Even the Justice Department knows that once something is in the operating system, any independent market for it collapses. Yes, security's time may well have come, but in a Warhol world, that would mean that it is about time to go.

The focus of "security" research today is the study of "trust management" --

how trust is defined, created, annotated, propagated, circumscribed, stored, exchanged, accounted for, recalled and adjudicated in our electronic world.

This is natural because security is a means and not an end.

This is mature

because all technology differentiates along cost-benefit lines.

All the

security technology that you can buy today enables some aspect of trust

management and novel variations show up daily.

You can walk out of this hall and buy systems that use passwords that get

local machines to trust you enough to let you in. You can buy smart cards

that can do your cryptographic calculations for you, respond to challenges,

hold your keys inviolable or, more interestingly, have identities of their

own and serve merely to introduce you on their own terms. You can buy

biometric devices that look at your voice, your face, your retina, your

fingerprint, or even the idiosyncrasies of how you learned to type and so

say, "Yep, that's the guy." You can get systems that are sufficiently

hardened that you can rely on them if for no other reason they

are so nearly
useless no one would want to break in. You can still get your
hands on
security systems in the raw and roll your own directly from
source-code.
You can, anywhere, anytime, spin-up virtual private networks
that are
trustworthy protectors of your confidentiality however hostile
the
intervening wires are. You can even deliver privacy between
strangers --
nearly a matter of creating trust in order to propagate it. You
can put a
document into the Eternity Service and trust that it can never
be erased or
you can put it into a cryptographic file system and trust that
it can never
be found. Simple? Yes; academics and entrepreneurs alike are
busy supplying
ways to propagate trust.

They have it all wrong.

If you ever took a course in probability then you know that many
problems
are solved by calculating their dual -- the probability of "not
X" can be a
whole lot more tractable than figuring $\Pr(X)$ directly. If
you're in a
security-based startup company, then you'll know that making
money requires
making excitement, even if the excitement is somebody else's
public
humiliation. And all of you can agree that the more important
something is,
the more it must be managed. Trust management is surely
exciting, but like
most exciting ideas it is unimportant. What is important is risk
management,
the sister, the dual of trust management. And because risk
management makes
money, it drives the security world from here on out.

Every financial firm of any substance has a formal Risk Management Department that consumes a lion's share of the corporate IT budget. The financial world in its entirety is about packaging risk so that it can be bought and sold, i.e., so that risk can be securitized and finely enough graded to be managed at a profit. Everything from the lowly car loan to the most exotic derivative security is a risk-reward tradeoff. Don't for a minute underestimate the amount of money to be made on Wall Street, London and/or Tokyo when you can invent a new way to package risk. The impact of Moore's Law on the financial world is inestimable -- computing has made that world rich because it has enabled risk packaging to grow ever more precise, ever more real-time, ever more differentiated, ever more manageable. You don't have to understand forward swaptions, collateralized mortgage obligations, yield burning, or anything else to understand that risk management is where the money is. In a capitalist world, if something is where the money is, that something rules. Risk is that something.

Security technology has heretofore been about moving trust around as if risk is definitionally undesirable and reliable trust management simply obviates the issue of risk. It does not come close. In two years time the "trust-hauling" market will be somewhere on the down-slope between legacy and dead. Risk management is going to take over as the dominant paradigm because risk management can subsume trust, but trust management cannot subsume risk. The Internet has made this so.

The Internet is irresistible because it lowers barriers to entry on a global basis -- global in both space and time. Ever more important parts of the world's economy exist only in cyberspace, and lead times have entirely collapsed. Every professional fortune teller is bidding geometric increases in the dollar volume of electronic commercial activity. But when there is enough booty available, even absurdly difficult attacks become plausible. This is the world we are in. It will never be possible to really do the job of trust management any more than it is possible to really win an arms race or really preclude your car from being stolen. But risk management -- that is doable and it is doable at a profit. The proof is all around us.

We are a score of years down this road. 1978 was a vintage security year; the remarkable papers by Rivest, Shamir & Adleman and Needham & Schroeder were published, both in CACM as it happens. The former introduced public key ideas and the latter created Kerberos. The counterpoint between these two technologies is instructive. Both symmetric cryptosystems, like Kerberos, and asymmetric cryptosystems, like RSA, do the same thing -- that is to say they do key distribution - -- but the semantics are quite different. The fundamental security-enabling activity of a secret key system is to issue fresh keys at low latency and on demand. The fundamental security-enabling activity of an asymmetric key system is to verify the as-yet-unrevoked status of a key already in circulation, again with low latency and on

demand. This is key management and it is a systems cost; a secret key system like Kerberos has incurred nearly all its costs by the moment of key issuance. By contrast, a public key system incurs nearly all its costs with respect to key revocation. Hence, a rule of thumb: The cost of key issuance plus the cost of key revocation is a constant, just yet another version of "You can pay me now or you can pay me later."

Because of the tradeoffs between who pays for what part of the systems cost and who gets the benefit, secret key systems and public key systems have different fields of use. Secret key systems are fast and offer revocation at no marginal cost. Public key systems are slow but they enable digital signature and thus enable proof of action, non-repudiation as it is called. Secret key systems are the default choice within an organization while public key systems are the default choice between organizations, i.e., secret key for where security is an intramural concern intramurally arbitrated, and public key for where security is extramural thereby requiring recourse to a third party judge in cases of dispute. The relentless blurring of what is intramural and what is extramural will favor public key over time.

Because a trust management paradigm says that a digital signature is only as valid as the key (in which it was signed) was at the moment of signature, it is only as good as the procedural perfection of the certificate issuer and the timely transmission of any subsequent revocation. **These

are high costs.** In fact, the true costs of general public key infrastructure are so extraordinarily high that only our collective ignorance of those costs permits us to propel ourselves toward a general PKI as if it were a panacea. When, not if, the user community at large realizes this, we "security people" will have but two choices, compromise on (gloss over) the quality of trust that public key can deliver or back off from the claims of full trust cheap. In other words, we'll have to fit the benefit to the endurable cost or fit the cost to the requisite benefit. Since, as a rule of thumb, to halve the probability of loss you have to at least double the cost of countermeasures, any finite tolerance of cost means an upper bound on how much security you can get. In the fullness of time, security technology will be evaluated on the same cost-benefit-risk tradeoff on which other technologies are evaluated. This is the price of maturity; this is the price not yet paid.

Do not misunderstand me; public key technology, secret key technology, security technology in general are daily reaching new levels of protective capability. What they cannot protect against is being over-sold, and they are being over-sold. Why is that?

The days when the Internet was a toy are gone even if a high percentage of its new investors are still coming in merely to avoid looking dowdy. The real question on the table is: When does the Internet become more like the

data center. And what does making the Internet more like the data center mean? At a minimum, it means metered use. Discussions are already widespread about requiring Internet postage; large ISPs will probably demand it, existing postal services would love to sell it and data centers, such as the financial giants, will get a better handle on what goes in and out the door. At least one Wall Street bank already does charge-back for network bandwidth consumption and their internal electronic security regime plays a role in assigning those costs just as, in turn, their security group manages the user database via incremental updates rather than fresh full copies so as to minimize their bandwidth charges. That's not postage, but it is close and it is now.

Incremental use charges are but one example, interesting mostly because they are a near term step toward making the Internet into a data center. The fundamental value of the data center is the information it holds. The past few years have seen data warehousing, data mining and now connection of the data center to the Web, data publishing if you will. MVS, for example, has a really good web server and someone in the audience will have to convince me that there is a difference between a 1970's central time-share machine and an MVS web server in a swarm of "thin clients" on fast networks. It certainly isn't the direct wire connection -- SSL simulates that well enough. It surely isn't the management model; the MIS director who had declared defeat in desktop configuration management will, you

can be sure,
rejoice at getting control back.

In the mainframe world, you move the computation to where the data is. In a client server world, you move the data to where the computation is. Web servers front-ending corporate databases attached to virtual private networks full of some universal client like a web browser sure sounds like a resurgence of the data center to me. The IBM 390 is a good machine and the Wintel cartel has pretty much ensured that no upstart will enter their space. From Wintel's point of view, using all those desktop cycles for display functions is just fine. Could it be that simple?

Financial markets made SUN what it is today and vice versa -- SUN's first big win, the first big demonstration that computing power had risen to such a degree that moving the data to where the computing is made sense, "the network is the computer" and all that. Financial markets, in the sense of traders going head to head, used that power to replace whom you knew with what you know and set off a technology-as-weapon metaphor that has overtaken most of the business world. Financial Markets, in the sense of Exchanges, now rely on a dense spread of computing that exceeds what most of us have to deal with; more than one major bank has 15,000 FTP jobs a night just moving data to or from its data center. Plenty of staff at the NYSE lose \$1000 apiece for every 15 minutes the Exchange is late opening due to IT unavailability. No computing equipment is too expensive when trumped with "I

can make that back on the first trade." No small country runs its currency anymore.

There was once no question that the fundamental purpose of an exchange was to provide "an advantage of time and place" to those who would trade on it and, in so doing, establish efficiency and liquidity baselines against which others would be judged. Beginning first with the "Paperwork Crisis" in the 60's and reaching a crescendo after the "Crash of '87," the Exchanges have been fully committed to electronic commerce before that phrase meant anything. But since the Internet, time and place are meaningless and the Exchanges know it. They are working hard to make oversight, fair play and quality of service into new baselines. Clearly, security technology is #1 in their list of requirements followed closely by scalability and integration.

Security in a financial world market that is both nowhere and everywhere is a difficult thing to define well enough to solve, but if there is anything to engineering as a discipline then it is that the heavy work is in getting the problem statement right. So, to return to my central premise, if new security technology is a result of investment and if the investment in security technology is naturally centered within the financial community, what is the problem statement? ** If we get that right, we can predict the future. **

I submit that the problem statement is how to bring a transactional semantic

to the Internet. This is not a new problem, but it is an as yet unsolved one. The existing financial markets want transactions because transactions are what they are about and transactions are what they know. Upstarts like the payment vendors want to be the first to deliver transactions and disintermediate the financial firms. Technical legal beagles reason that there is no transaction without recourse, no recourse without contract, no contract without non-repudiation and no non-repudiation without digital signature. Anyone who wants to do business on the Web needs transactions.

Hal Varian, an economist and Dean of the Information Management School at Berkeley, taught me that what the Internet changes more than anything else is that it brings the efficiency of auction to markets that never had that option. This is a cover story in this week's "The Industry Standard." Auctions need security technology because what makes an auction an auction is the ability to conclude a transaction which, by its own execution, "discovers" a price. In other words, the nature of the world's economy is changed by the existence of the Internet, but only on the condition that electronic transactions are up to job.

So what do I mean by "transaction?" I mean a non-repudiable communication between two parties who can each verify the time-, value- and content-integrity of that communication, who can presume confidentiality of that communication, who can verify the authenticity and authorization of their counterparty and who can present all these evidences to

third party
adjudication should there be a need for recourse at any
arbitrary time in
the future. **Every single part of that definition begs the
question of
security mechanism.** It is on that basis I claim that the
security
technology of tomorrow will be crafted in response to the unmet
needs of
financial markets today.

As an example, your handwritten signature on a check is what, in
principle,
authorizes that funds move from A to B. In truth, from a bank's
point of
view, actually verifying handwritten signatures is a transaction
cost that
is not worth bearing unless the cost of verification is less
than the risk
of loss. At the largest banks, the threshold dollar amount below
which
verification does not really happen is a closely guarded number,
but it
generally exceeds \$20,000 and still they have platoons of people
doing this
all day, every day. Converting the means of signature
verification from a
manual process into a machine-able one would radically change
the economics
of check processing. It would add billions to bottom lines and
do it from
the cost-avoidance side of the ledger.

But that is not all. Some \$300B of U.S. payments are made every
day of which
only \$60B are in the form of checks; the balance is largely in
cash
transactions of \$5 or less. From both the merchant's and the
bank's
perspectives, getting rid of cash would be a huge win because
handling costs
for small dollar amounts often exceed the profit margins on the
underlying

sales. While the consumer may well adopt cashless payment out of some sense of convenience, the financial side of the house will enable it to avoid costs.

Only this morning, Frost & Sullivan released a study that defines e-commerce as "commercial transactions taking place over the Internet with exchange of value in real time." Web payment sparked numerous startups with numerous different mechanisms. It is too late for you to enter this market, but it is not too late for those payment-systems vendors to rethink what they are trying to do. All of them are suffering because the volume of Web-based retail business has not picked up as fast as their business plans had presumed. For the retail customer, the main thing the Web offers is product discovery; a good print catalog and an 800 number are otherwise hard to beat. It is clear that the real money in Web commerce is in business-to-business commerce, but there the supply chain has a lot more complication and the kinds of security mechanisms need to be better than those for buying a toaster oven. Whereas retail commerce is about small dollar amounts and stranger-to-stranger transactions through a financial intermediary like a credit-card company, business-to-business is more about relationships, the dollar value of the sale is much bigger, and banks play a direct role (through letters of credit, collateralized bills of lading, etc.)

B2B commerce does not have a good solution yet. If you want to sell into

this market, be aware that the customer will buy either to avoid costs he has now or to make revenue he doesn't have yet. In the case of saving costs, you'll have to sell him the technology on a turnkey basis - -- he will not cut you into the transactional revenue stream. If you can really show that your technology will make him revenue he did not have a chance to make otherwise, you may be able to get a piece of the revenue stream, but do not underestimate the cost-avoidance focus of big buyers and sellers. As far out as 2005, over half the Internet-transactions will be transactions converted from paper and credit/debit cards, not new transactions. **When selling into a cost-averse market you automate rather than revolutionize, and you do not get a piece of the action.**

Everyone likes to talk about "disintermediating the banks," that is making the intermediary role of banks in commerce less essential by performing that service in some other way. Bill Gates is widely quoted as saying that "Banks are dinosaurs." At the highest end, they are not dinosaurs and they are not about to be disintermediated. Whilst the banks have a natural affection for their income streams, that doesn't prevent disintermediation. Most wiseguys trying to disintermediate the banks misunderstand what banks do. This is what they do: They interpose their balance sheet between the expectations of the counterparties to a transaction and the risk of default on either of their parts. They undertake stop-loss protections against credit risk, insolvency, operational failure, currency fluctuation, diversion

of funds
delivery, etc. In other words, they manage risk because they can
absorb
loss. ****Electronic commerce payment technology cannot absorb
loss, so it
cannot and will not disintermediate the banks.****

Think of this this way: All public key technology is driven to
make a
digital signature verifiable, i.e., it is about quality control
and
guarantee on the signature itself. This is a stunning thing, but
it is not
the whole equation. The intermediation role that banks play is
to guarantee
the transaction, i.e., it is broader than just the verification
of a
signature. The bank's know-how and its balance sheet are not
something that
can be replaced by a cryptographic calculation. The ability to
avoid loss
never makes up for the ability to absorb loss. The cryptography
guarantees
the signature; the bank's capital guarantees the transaction.
****Risk control
encapsulates trust.****

In the midst of this, you might say "What are the standards?" in
the
sense of "What do the formal standards groups have to say?" The
banking
world is regulation rich and standards rich, too, which begs the
question -- "Which standards matter?" The world of the Internet
is
making some of the banking-centric standards passe' but, unlike
the
combination of standards and regulations the banks are familiar
with,
the standards groups of the Internet cannot take on
accountability for
the implications of conformance/non-conformance though they
continue to
define it for others. This makes Internet standards substantially

difficult to swallow because there is no accountability, nor can there be. The absence of enforcement guarantees that the only Internet standards that will really get attention are those that promote interoperability across jurisdictional boundaries. Ironically, this is all the pioneers of the Internet ever wanted.

What the banks want, and I assure you they will get, is a set of cryptographically sophisticated tools that move the risks of the Internet from open-ended to estimable. In a sense, this is like insurability. It is probably apocryphal, but the story goes that a major investment firm with a Web commerce idea went to a big insurance company to seek stop loss protection. The conversation supposedly went like this:

"How big is the potential loss?"
"We don't know."
"How likely is a loss to occur?"
"We don't know."
"How much is your company worth?"
"This much."
"That's the premium; send it in."

Whether true or not, it illustrates the point -- the issue is getting a handle on the risk such that it can be priced. Every one of you who has tried to sell security technology has discovered that the only willing customers are those who either (1) have just been embarrassed in public or (2) have just learned that they are facing an audit. Everyone else is an unwilling customer. We've been dumb about this; we've tried to sell security as a means to establish trust but we've done it by railing about threats. It's no damned wonder that we haven't sold much. I know I have

often wondered if my market might not explode were I to get just one of the big loss-prevention insurers to make good security practices and technology into an underwriting standard. Then, just like "Do you have sprinklers?" everyone is forced to confront whether they want to pay for security or pay for non-security. I am confident that the insurers could soften up my targets a lot better than I can.

Let me tell you, they are about to. Insurability of Web commerce is essential, and no insurer is going to accept "We don't know" as an answer. They will say "Send it all in" and they'll mean it. The demand side for security technology is exploding but it isn't quite the security technology we have on hand.

If a digital signature has the uniquely irreplaceable property of providing proof to a judge, then the role of a "trusted third party" is going to become more important over time, not less. Think of it this way: when I get a certificate issued to me by a certifying authority, I do have some risk around whether the CA is well operated or not. This includes the probability they will issue a certificate with my public key but someone else's name and whether when I tell them that my key has been compromised they will spring into decisive action. Most of that risk I can handle by a combination of due diligence and contract.

However, when I give my certificate to you and say "Hi, I'm here from Central Services to fix your system" it is you that's in a risky

position. You have to say "Is this certificate valid?" That means you have to check that the certificate is not listed as revoked, that the signature on the certificate is well formed, that the certificate authority which issued this certificate itself has an identity certificate that is itself validly signed, that the certificate authority is itself not in any trouble with revocation, and and so forth, ** recursively. **

The full cost of revocation testing is proportional to the square of the depth of the issuance hierarchy. In other words, this exceeds the intellectual capacity of most certificate recipients. This means that most recipients cannot themselves rely on the security technology to establish trust beyond the shadow of doubt. Instead, if recipients are smart, they will turn again to the insurance world just as risk holders have done whenever they cannot afford to carry on their books the consequences of a remotely unlikely event. For the insurer, he will underwrite a guarantee on the transaction for a fee that will reflect his experience with the CA's practices, the kind of transaction undertaken, the dollar amounts involved, etc. This will seem sensible to all parties because it is so familiar. This is risk management underwritten by financial intermediaries. This is where we will shortly be. This is the card eight major banks and CertCo played ten days ago -- the formation of "a global network of compliant businesses that use a common risk management framework." **This is where we securitize the transactional risk of electronic commerce.**

There is one potential fly in this ointment, and I do not intend to dwell on it, but I cannot get this far and not mention the threat to strong security apparati of having them undermined by key escrow. Corporate policies and laws alike have always been defined in a territorial way that relies on clearly identifiable borders, physical locations where the policy or the law come to an end. But in the electronic world borders are meaningless. In some sense, sovereignty, based as it was on the idea of a border, is less meaningful now than for some centuries. In its place is a different kind of sovereignty, because the only borders in an electronic world are cryptographic ones. As such, the debate over who may or may not have a key known only to themselves is a proxy discussion for who may or may not have sovereignty within a cryptographically defined space.

There are hard questions yet to answer. Compromised keys are revoked effective not to the moment of suspicion of compromise but rather retroactively to the last known time when the key was safe. In the case of escrow, should not a key's owner retroactively revoke it to the moment of its seizure from escrow should the owner later discover that it has been so seized? Or if a revoked key is only revoked by the action of the certifying authority signing a revocation notice in a special key, can that revocation-signing key itself ever be revoked? If it could, would that not invalidate (reverse) any revocations signed in it and what does that mean? I only offer these so that you do not equate my argument about the near-inevitability of investment in public key technology and digital-signature-dependent activities with some presumed

infallibility of
the technology or our understanding of it. These questions will
be settled
one way or another, but they remain open as we speak here today,
and there
is money to be made.

I have tried to lay out my estimation on which way the tide is
running and
which moon's gravity matters. I could be completely wrong, or
merely
overstating what my biases bring me, but I think not. I think
that just as
the best estimate of tomorrow's weather is today's, the best
estimate of how
the Internet and the financial behemoths will interact is for
the Internet
to be driven, as a side effect, by the cost-reduction and profit-
incented
strategies of those financial behemoths. They already transcend
national
boundaries and their investment decisions do run the world.
Were this to
get enough investment, it might make security a solved problem
at least as I
define "solved" to mean "consistent with risk management in the
insurance
style." Since that would collapse the market for novel security
add-ons, I
strongly suggest that as you prepare your business plans you
figure out how
to be, as Tom Lehrer would say, a doctor specializing in
diseases of the
rich.

This is a very exciting time and it is a privilege to be a part
of it. When
we are all relics in rocking chairs, we will still know that we
were present
at the creation. I know that I will count myself particularly
lucky,
including for your close attention these past few minutes.

Thank you for the honor of speaking with you.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 7

Saturday 14 November 1998

Contents

- [Lovesick cod overload submarine sonar equipment](#)
[Christoph Conrad](#)
- [O'Hare's radar malfunctioning](#)
[Doneel Edelson](#)
- [Dallas-FortWorth ARTS air-traffic control upgrade backed out](#)
[PGN](#)
- [NASAA spam investors by mistake](#)
[Mich Kabay](#)
- [Interference risks on cruise missiles](#)
[Gordon Lennox](#)
- [Talking elevator with off-by-one error?](#)
[George Michaelson](#)
- [3Com Security Advisory: We built in back doors, so you're at risk!](#)
[John Gilmore](#)
- [Re: Unreliable reception of e-mailed WP documents](#)
[Garth Anderson](#)
- [Re: LA 911 Outage](#)
[John Sheckler](#)
- [Business jet trips/privacy](#)
[Daniel P.B. Smith](#)

- [Corrections on recent issues](#)
[PGN](#)
 - [GPS internal clock problem](#)
[Bob Nicholson](#)
 - [Dumbing down English speech](#)
[Bertrand Meyer](#)
 - [REVIEW: "Cyberspace and the Law", Edward A. Cavazos/Gavino Morin](#)
[Rob Slade](#)
 - [REVIEW: "E-Commerce Security", Anup K. Ghosh](#)
[Rob Slade](#)
 - [System Safety Society Conference -- Call for Papers](#)
[Dixon Jack](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Lovesick cod overload submarine sonar equipment

Christoph Conrad <Christoph.Conrad@post.rwth-aachen.de>

Fri, 13 Nov 1998 21:42:20 +0100

Associated Press in a German newsletter, 13 Nov 1998
(retranslated by me):

"Norwegian submarines have discovered an unexpected problem while diving off the Norwegian coast: the grunting noise from swarms of lovesick cod overburdens the sonar equipment. Thereby navigation in Norwegian waters is almost impossible, said the Defense Department yesterday."

Christoph.Conrad@post.rwth-aachen.de

[For non-English readers, codfish = torsks in Scandinavian languages, while other linguistic fish roots stem from bacalao, morue, merluzzo, Kabeljau, tara, ... For English speakers, it is evident that the

submarines need a cod peace to hide their attractive nature.
PGN]

✶ O'Hare's radar malfunctioning

"Edelson, Doneel" <doneeledelson@aciins.com>
Thu, 29 Oct 1998 12:42:10 -0500

Air-traffic controllers say a new radar system has been malfunctioning, causing them to lose track of planes at O'Hare International Airport, one of the world's busiest airports. The computer system repeatedly drops critical flight information, misidentifies aircraft location, and gives false information, according to Kurt Granger, president of the National Air Traffic Controllers Association in Elgin, Illinois. Federal Aviation Administration spokesman Don Zochert denied Granger's claims, saying the new system is safe. He said the new, up-to-date software is also used in Denver, Dallas and New York City. [Source: *USA Today*, 29 Oct 1998]

✶ Dallas-FortWorth ARTS air-traffic control upgrade backed out

"Peter G. Neumann" <neumann@csl.sri.com>
Wed, 11 Nov 1998 11:26:35 -0500

The ARTS 6.05 software in use at the DFW regional TRACON (Terminal Radar Approach Control) center has been causing so much confusion for the

controllers (who maintained that safety was compromised, whereas the FAA and the union had said there was no danger) that the system has been backed off to an earlier version, ARTS 6.04. Reportedly, there some ghost (nonexistent) aircraft showing up, while real planes were omitted. Controllers noted that 200 complaints in the past month had been ignored by the FAA until now. One particular case occurred on 30 Oct 1998, when a flight disappeared for 10 miles. Another case involved a plane at being handed off at 10,000 feet, with the recipient controller's screen showing the plane at 3,900 feet. Such problems had not occurred with ARTS 6.04, but ARTS 6.05 seems to have significant improvements (ignoring the glitches).

This is the same software that is used in Chicago (see the previous item in this issue!), Denver, NY, and southern California.

``Officials compared the shift between the two programs to the difference between the Windows 95 and Windows 98 operating systems on personal computers. As with any new software, there are bugs to be worked out, they said.'' [That is REALLY reassuring. PGN]

[Source: article by J. Lynn Lunsford, *Dallas Morning News*, 7 Nov 1998, and an article by G. Chambers Williams III, Fort Worth Star Telegram, 7 Nov 1998; the quote relating to Windows 95/98 is from the FW Star Telegram article. PGN Stark Abstracting]

✶ NASAA spam investors by mistake

Mich Kabay <mkabay@compuserve.com>

Mon, 2 Nov 1998 11:09:53 -0500

Anti-fraud vigilantes responded to an appeal from the North American Securities Administrators Association (NASAA) for leads on possible securities fraud involving junk e-mail. Unfortunately, last week (30 October), these good citizens each received up to 300 messages thanking them for their tip. The glitch was solved by Friday morning. Anyone wanting to contribute to the fight against stock fraud is invited to visit the NASAA web site at <<http://www.nasaa.org>> for information on how to participate.

[Source: a Reuters item , 31 Oct 1998]

M. E. Kabay, PhD, CISSP / Director of Education

ICSA, Inc. <<http://www.icsainc.net>>

✶ Interference risks on cruise missiles

<Gordon.LENNOX@BXL.DG13.cec.be>

Wed, 4 Nov 1998 13:25:20 +0100

Following the Patriot item...

> From Aviation Week & Space Technology - 2 Nov 1998 - Page 23

> The auctioning of frequency spectrum to commercial telecommunication

> providers is undermining the Pentagon's ability to counter low-observable

> (LO) cruise missiles.... The large amount of spectrum already auctioned off

> even now is impacting at least one classified system used to detect

> low-observable aircraft and missiles...

[... not to mention the Leonid shower of meteorites coming up in a few days. PGN]

⚡ Talking elevator with off-by-one error?

George Michaelson <ggm@dstc.edu.au>

Thu, 12 Nov 1998 11:19:10 +1000 (EST)

new building. 7 floors labelled [1..7]

enter lift [elevator]. select floor 1.
arrive at floor 1. lift announces:
"floor eight"

My guess is that the software is generic and is loosely coupled to the real

"I know where I am" function the lift has innately, talking or not. I have a mild concern that a lift this confused maybe doesn't want to be used.

Shades of Douglas Adams..

-George

⚡ 3Com Security Advisory: We built in back doors, so you're at risk!

John Gilmore <gnu@toad.com>

Wed, 28 Oct 1998 12:08:25 -0800

They don't quite admit to not knowing anything about security --

putting
undocumented back-door passwords into their switches, and
putting in a way
to read the administrator's password via an un-authenticated
SNMP query.
But you can tell that the information secured by this incredible
obscurity
is all over the cracker community, if 3Com is now willing to put
it up on
their Web page. As usual, only when the bad guys have had your
system wide
open for months, will the supposed "good guys" tell you, ahem,
you have a
problem. They *did* release fixed firmware, I give them credit
for that.

John

<http://www.3com.com/news/advisory51498.html>

> 3Com Security Advisory for CoreBuilder and SuperStack II
customers
>
> 3Com is issuing a security advisory affecting select
> CoreBuilder LAN switches and SuperStack II Switch products.
> This is in response to the widespread distribution of special
> logins intended for service and recovery procedures issued
> only by 3Com's Customer Service Organization under conditions
> of extreme emergency, such as in the event of a customer
> losing passwords.
>
> Due to this disclosure some 3Com switching products may be
> vulnerable to security breaches caused by unauthorized access
> via special logins.
>
> To address these issues, customers should immediately log in
> to their switches via the following usernames and passwords.
> They should then proceed to change the password via the
> appropriate Password parameter to prevent unauthorized access.
>
> * CoreBuilder 6000/2500 - username: debug password: synnet
> * CoreBuilder 3500 (Version 1.0) - username: debug password:
synnet

```
> * CoreBuilder 7000 - username: tech password: tech
> * SuperStack II Switch 2200 - username: debug password:
synnet
> * SuperStack II Switch 2700 - username: tech password: tech
>
> The CoreBuilder 3500 (Version 1.1), SuperStack II Switch 3900
> and 9300 also have these mechanisms, but the special login
> password is changed to match the admin level password when the
> admin level password is changed.
```

[Here's the best part:]

```
> Customers should also immediately change the SNMP Community
> string from the default to a proprietary and confidential
> identifier known only to authorized network management staff.
> This is due to the fact that the admin password is available
> through a specific proprietary MIB variable when accessed
> through the read/write SNMP community string.
>
> This issue applies only to the CoreBuilder 2500/6000/3500 and
> SuperStack II Switch 2200/3900/9300.
>
> Fixed versions of software for CoreBuilder 2500/6000/3500 and
> SuperStack II Switch 2200/3900/9300 are available below.
>
> General administration of these systems should still be
> performed through the normal documented usernames and
> passwords. Other facilities found under these special logins
> are for diagnostic purposes and should only be used under
> specific guidance from 3Com's Customer Service Organization.
>
> For more information 3Com has dedicated a hotline at
> 1-888-225-1733. Outside the United States please contact your
> local Customer Service Organization location.
```

⚡ Re: Unreliable reception of e-mailed WP documents ([RISKS-20.03](#))

<Outla@aol.com>

Wed, 14 Oct 1998 14:08:10 EDT

The blank-field problem is a well-known and well-understood bug that is much more general than which word processor or OS or software version is being used. It happens wherever text is displayed in a field, column, cell, or window on a screen. The most common fix is to make all fields a bit larger than seems necessary, just to account for variations on different machines.

Text windows generally make the bottom line blank if that line doesn't completely fit in the window. The purpose seems to be preventing users from seeing only the top half of any letters. There are reasons for this beyond convenience, speed, or aesthetics: the top halves of i and j look identical, as do v and y. It's quite possible to program a window to display a partial line, and many do, but that is a very common default.

Fonts are interpreted and displayed by the local machine. Sometimes the original font is unavailable; sometimes the font is adjusted to fit the screen resolution or printer resolution or user preferences or even converted to bold or italics. If such conversion leads to a screen font taller than the field in which it will be displayed, then even the first line of text will be blanked.

Note that the field or box which holds the text is itself drawn a subtly different size on each computer; even if the font converts exactly, some screens might still see a blank field. Also, even if you view (and print) the

document on every configuration available there could still be surprises at run-time: the text may be reformatted temporarily, such as when the field is being edited or is made read-only.

The RISK is that this default behavior is very unexpected in fields designed to display only one line of text, even when it is accepted as normal in multi-line text fields. The unexpected results can easily lead to miscommunication.

Garth Anderson <Outla@aol.com>

⚡ Re: LA 911 Outage (Maufer, [RISKS-20.03](#))

<sheckler@SOFTWARE.ORG>

Wed, 14 Oct 1998 13:46:29 -0400

Here is how **The Washington Post** reported it. Interesting how the cause seems to have differed considerably. I suspect that they were describing the electricians' version of a high-temp hand-held blower for shrinking tubing and other heating purposes. These things are commonly called "hair dryers" only because they vaguely resemble one.

L.A.'s 911 System Is Back in Service, **The Washington Post**, from news services 12 Oct 1998; Page A10; Nation in Brief
<http://search.washingtonpost.com/wp-srv/WPlate/1998-10/12/0591-101298-idx.html>

Workers using hair dryers to clean hundreds of delicate circuit boards brought the city's 911 system back on line yesterday after

sprinklers
flooded a communications room. A backup system kicked in and
rerouted
emergency calls to individual police stations during the 17
hours that power
was shut off to the dispatch center. Sprinklers put out a fire
Saturday
afternoon in a storage room below City Hall, but 2,000 gallons
of water
seeped down and soaked ceiling-high racks of circuit boards that
link 911
operators to area emergency dispatchers. "There were cables
floating in six
inches of water. That's the kiss of death. People aren't even
allowed to
drink coffee at their desks because they could spill it," said
supervisor
Monika Giles. "We're lucky it came back on at all." [...]

John Sheckler, CQA, Software Productivity Consortium, 2214 Rock
Hill Road,
Herndon, VA 20170-4227 703-742-7156 <http://www.software.org>

Business jet trips/privacy

"Daniel P.B. Smith" <dpbsmith@world.std.com>
Sat, 31 Oct 1998 10:41:31 -0500 (EST)

Sorry, don't have the article at hand... hope others will give
more
details... there was an article in last week's Wall Street
Journal--front
page, that third-column-from-right "feature" story--that says
that the
TheTrip.com web site tracks not just commercial flights, but any
flight
for which you know the aircraft's tail number, and that there's
some other
site where you can look up the tail number. The result is that

anyone can
track the flights of any corporate jet.

One corporate critic put this to use to get strong
circumstantial evidence
of expensive junketing ("I don't know any Fortune 500 companies
with
headquarters in The Hamptons.") Obviously this information can
also be used
for industrial espionage and by stock traders (hmmm, what's
Sledge-O-Matic
Software Systems' plane doing in Seattle?).

The story wasn't completely clear on whether this information is
supposed
to be public. The impression I got it that it is another
example of
information that _is_ supposed to be public but suddenly
everything looks
different when public access is widespread, easy, and cheap.

To this naive individual, the most interesting sidelight was the
revelation
that the reason why companies bear the expense of corporate jets
is not
convenience, timeliness of flights, nor the desire to save
precious minutes
of time for individuals whose time is worth hundreds of dollars
per minute,
but the supposed secrecy of the flights.

Daniel P. B. Smith <dpbsmith@world.std.com>

✶ Corrections on recent issues

RISKS List Owner <risiko@chiron.csl.sri.com>
Sat, 14 Nov 1998 11:21:12 -0500

Too much traveling recently and too little time for RISKS.

I messed up in preparing [RISKS-20.05](#).

Sensormatic of course makes the anti-theft device, not defibrillators.

BADREF.

I messed up in preparing [RISKS-20.06](#).

The month at the top of the issue was OFF-BY-ONE.

Both corrections are noted in the respective catless and sri archive copies.

I was hoping to put this issue out on Friday the 13th (yesterday), but perhaps it is just as well I had no time!

[Which reminds me I just saw a note saying that a now-retired British vicar, Reverend Leslie Robinson, claims that the 1989 Kegworth air disaster in which a London-Belfast plane crashed onto the M1 highway, killing 47 and injuring 79, was influenced by a witches' coven operating under the flight path. The good engine had been turned off, instead of the malfunctioning one. Rebuttals are also included. *Yorkshire Evening Press*, 12 Nov 1998]

I wonder how many problems RISKS will have because of Y2K? (I'll be back in WashDC during the coming week for another meeting of the General Accounting Office Executive Council on Information Management and Technology, dealing with the U.S. Government's Y2K preparedness -- or lack thereof. Progress still seems to be much slower than it ought to be. Check out Congressman Stephen Horn's cumulative report card at <http://www.house.gov/reform/gmit> .)

PGN

✈ GPS internal clock problem

"Bob Nicholson" <lattice@popmail.dircon.co.uk>

Wed, 11 Nov 1998 08:20:39 +0000

[This has been reported earlier, beginning in [RISKS-18.24](#), but is still a problem. PGN]

As a licensed aircraft engineer, I regularly receive "AIRWORTHINESS NOTICES" from the British CAA. Here is one (verbatim) that may be of interest.

CIVIL AVIATION AUTHORITY : o

AIRWORTHINESS NOTICE

No. 7*

Issue 1

23 October 1998

THE POTENTIAL RESETTING OF GLOBAL POSITIONING SYSTEM (GPS) RECEIVER INTERNAL CLOCKS

1 Introduction

1.1 The timing mechanism within GPS satellites may cause some GPS equipment to cease to function after 22 August 1999 due to a coding problem. The GPS measures time in weekly blocks of seconds starting from 6 January 1980. For example, at midday on Tuesday 17 September 1996, the system indicates week 868 and 302,400 seconds. However, the software in the satellites' clocks has been configured to deal with 1024 weeks. Consequently on 22 August 1999 (which is week 1025, some GPS receivers may revert to week one (i.e. 6

January 1980).

1.2 Most airborne GPS equipment manufacturers are aware of the potential problem and either have addressed the problem previously, or are working to resolve it. However, there may be some GPS equipment (including portable and hand held types) currently used in aviation that will be affected by this potential problem.

2 Action to be taken by Aircraft Operators Aircraft operators, who use GPS equipment (including portable and hand held types), as additional radio equipment to the approved means of navigation, should enquire from the GPS manufacturer whether the GPS equipment will exhibit the problem. Equipment that exhibits the problem must not be used after 21 August 1999 and either be removed from the aircraft or its operation inhibited.

For the Civil Aviation Authority, Safety Regulation Group,
Aviation House,
Gatwick Airport South, West Sussex RH6 OYR

⚡ Dumbing down English speech

<Bertrand.Meyer@eiffel.com>

Tue, 10 Nov 98 14:40:31 PST

Although complaints about Microsoft Word's eagerness to correct what it sees as mistakes are not new in RISKS, I think it is still useful to protest vehemently the way Word 97 promotes the dumbing down of English writing by flagging (when you use its default options) any sentence which,

according to
some mysterious criterion, it deems too long, even if the
sentence is made
of several semicolon-separated clauses, and even though it is
perfectly
obvious to anyone, fan of Proust or not, that clarity is not a
direct
function of length, since it is just as easy to write obscurely
with short
sentences as with longish ones and, conversely, quite possible
to produce an
absolutely limpid sentence that is very, very long.

Bertrand Meyer, Interactive Software Engineering, Santa Barbara
<Bertrand.Meyer@eiffel.com>, <http://eiffel.com>

✶ REVIEW: "Cyberspace and the Law", Edward A. Cavazos/ Gavino Morin

"Rob Slade" <rslade@sprint.ca>
Thu, 29 Oct 1998 10:37:38 -0800

BKCYSPWL.RVW 980817

"Cyberspace and the Law", Edward A. Cavazos/Gavino Morin, 1994,
0-262-53123-2, U\$19.95

%A Edward A. Cavazos polekat@well.sf.ca.us

%A Gavino Morin gmorin@bga.com

%C 55 Hayward Street, Cambridge, MA 02142-1399

%D 1994

%G 0-262-53123-2

%I MIT Press

%O U\$19.95 +1-800-356-0343 fax: +1-617-625-6660 manak@mit.edu

%P 215 p.

%T "Cyberspace and the Law: Your Rights and Duties in the On-
Line

World"

"Net Law" (cf. BKNLHLUI.RVW) was written for the lawyer.

"SysLaw"

(cf. BKSYSLAW.RVW) was written for the layman, rather than lawyer, but was still aimed at sysops rather than the common herd. This book fills that space, and is the first I can recall that does so.

Chapter one provides a very brief description of cyberspace, starting with William Gibson's invention of the term, running through various different electronic entities, and including some basic online activities. Privacy, and particularly the Electronic Communications Privacy Act as applied to the Steve Jackson Games case, is the topic of chapter two. The chapter ends with a rather odd look at encryption. Eventually getting around to PGP's problems with ITAR (the International Traffic in Arms Regulations), the book seems to state that PGP should be avoided because simple possession of it may be illegal. Since the book is based entirely on US law, it is obviously aimed at an American audience, and the issue of export does not appear to be mentioned. Contracts are the subject of chapter three, mostly dealing with common law.

Chapter four covers copyright. I must say that I am always amused by the wording of the American First Amendment; that government shall make no laws regarding the abridgement of freedom of speech or press; since there are laws about defamation, fraud, and pornography. These, and free speech, are dealt with in chapter five. Considerations of prurient material are discussed in significantly more detail in chapter six, and I must say that

this is one of the most informative and even-handed explanations of the topic in any book reviewed to date. Chapter seven closes off the book with a grab bag of potentially illegal computer related activities. The intent seems to be to warn users about apparently innocuous actions that could bring them afoul of the law. As usual, there is a section on computer viruses, and, as usual, it isn't very good. Appendix A provides a good list of contacts for legal and paralegal interest groups. Other appendices list various US statutes examined in the book.

While this work once again limits itself to the US, and fails to note the international nature of cyberspace, it does provide its information in a readable and accessible form. The authors do not always deliver on their promise to avoid legal jargon (such as "color of law"), but all the contents can be understood by the intelligent and determined lay reader. Where legal niceties are not completely delineated they would only be of interest to other lawyers anyway.

copyright Robert M. Slade, 1998 BKCYSPLW.RVW 980817

✶ REVIEW: "E-Commerce Security", Anup K. Ghosh

"Rob Slade" <rslade@sprint.ca>
Thu, 5 Nov 1998 11:28:36 -0800

BKECMSEC.RVW 981003

"E-Commerce Security", Anup K. Ghosh, 1998, 0-471-19223-6,

U\$24.99/C\$35.50

%A Anup K. Ghosh

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 1998

%G 0-471-19223-6

%I John Wiley & Sons, Inc.

%O U\$24.99/C\$35.50 416-236-4433 fax: 416-236-4448

%P 288 p.

%T "E-Commerce Security: Weak Links, Best Defenses"

The title is ever so slightly misleading in that the topic is not electronic

commerce as a whole, but the (admittedly most popular) Web segment of it.

However, within this limit, the book does provide solid coverage and good

advice for a whole range of issues.

Chapter one is a general introduction to the factors involved, looking at

some recent "attacks" of various types, and then reviewing the client,

transport, server, and operating system components to be examined in the

remainder of the book. Client (generally browser) flaws are covered

thoroughly in chapter two. The breadth of coverage even includes mention of

topics such as the concern for privacy considerations with cookies. Active

content is the major concern, with an excellent discussion of ActiveX

(entitled "ActiveX [In]security"), a reasonably detailed review of the Java

security model, and a look at JavaScript. Unfortunately, very little of

this touches directly on e-commerce as such, except insofar as insecure

client technology is going to make e-commerce a harder sell to the general

public. While covering the transport of transaction information, in chapter

three, Ghosh makes an interesting distinction between stored

account systems
(where you want to secure the transmission of identification data) and
stored value systems (where the data, once transmitted, is
useless to an
eavesdropper). Many books concentrate on either channel
security or
electronic cash systems, so this comparison is instructive.

A server involves multiple programs, and may involve multiple machines.

Server security can quickly become complex, and this is quite evident in
chapter four. While a great deal of useful and thought-provoking information is presented, the complicated nature of the undertaking works
against this chapter. Not all topics are dealt with thoroughly, or as well
as the previous material was. Oddly, one issue not covered in depth is the
firewall, which is handled very well in chapter five, with operating system
problems. Ghosh sets up a classification scheme for OS attacks, illustrated
by specific weaknesses in Windows NT and UNIX.

The book ends in chapter six with a call for certification of software,
greater attention to security in all forms of software, and, interestingly,
for greater use of component software. (From the jacket material, it
appears that Ghosh is currently involved in the promotion of component
software systems.)

Each chapter ends with a set of references. Unlike all too many books with
bibliographies stuff with obscure citations from esoteric journals, the bulk
of the material listed is available on the Internet. (RISKS-FORUM Digest
readers may already have seen much of it.) A separate section

lists Web
sites used in the text.

The various issues dealt with in the book are explained clearly,
and

generally present counsel on the best practices for secure
online commerce.

A compact but comprehensive guide to the current state of
electronic
transaction security.

copyright Robert M. Slade, 1998 BKECMSEC.RVW 981003

✦ System Safety Society Conference -- Call for Papers

"Dixon, Jack" <jack.dixon@lmco.com>

Wed, 04 Nov 1998 14:58:23 -0500

System Safety -- System Safety at the Dawn of a New Millennium
17th International System Safety Conference
16--21 August 1999

Holiday Inn International Drive Resort
Orlando, Florida, USA

See <http://www.system-safety.org>

Abstracts due 15 Jan 1998.

Jack Dixon -- Technical Program Chair, ISSC1999@yahoo.com
P.O. Box 780660, Orlando, FL 32878-0660 USA Ph: (407) 306-5141.

Registration and Orlando Information:

CPS, Inc., 2453 Orlando Central Parkway, Orlando, FL 32809
(800) 777-5333, fax (407) 851-8313



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 8

Sunday 15 November 1998

Contents

- [Sweden recommends banning mobile telephones on ships](#)
[Heinrich Hetzel](#) via [Robert Hettinga](#)
- [*Very* hairy bug in Excel 4.0 and Excel 98...](#)
[Lindsay Marshall](#)
- [Identity theft defeated by victim's wife](#)
[Jim Griffith](#)
- [Electronic Commerce: The Future of Fraud](#)
[Bruce Schneier](#)
- [Password capturing](#)
[Bill Carton](#)
- [REVIEW: "Virus Alert of the Day", virus-alert@optimator.win.net](#)
[Rob Slade](#)
- [REVIEW: "VirusHelp", Henri Delger](#)
[Rob Slade](#)
- [Info on RISKS \(comp.risks\)](#)

⚡ Sweden recommends banning mobile telephones on ships

"Heinrich Hetzel" <hwh@email.com>

Sat, 14 Nov 1998 22:58:54 +0100

[Forwarded to RISKS by Robert Hettinga <rah@shipwright.com>. PGN]

The Swedish National Maritime Administration has recommended that shipping firms ban the use of mobile telephones aboard ships. In Norway recently, a man aboard a ship used a phone on the foredeck, at which time the ship's rudder suddenly swung hard over while the vessel was on autopilot. After the ship returned to its course, he again tried to use the phone and the autopilot again made a course change. It is believed that the phone's magnetic pulse interfered with the autopilot's operation. While Det Norske Veritas is studying the problem, Sweden is recommending such phones be banned for the time being.

Above copied from notice to mariners.

I had a few turns close to an airport, but I never found out what triggered them.

Anyone else with unexplained unexpected course changes?

From WORLD CRUISING SUBSCRIPTION PAGE - <http://window.to/worldcruising>

CHAT ROOM: <http://www.infohouse.com/amelia/cruisers-connection/wcchat.htm>

***Very* hairy bug in Excel 4.0 and Excel 98...**

<Lindsay.Marshall@newcastle.ac.uk>

Fri, 13 Nov 1998 10:14:50 +0000 (GMT)

This from Macintosh: <http://www.macintosh.com>

> We have verified a serious Excel bug reported on the Mac Managers mailing
> list today: If you have a hard disk and a floppy both with the same name,
> Excel will save a file onto the hard drive when you tell it to save to the
> floppy. Among other nasty problems, this may succeed in bypassing disk
> security controls provided by such programs as At Ease. More details:
> "Excel is the only application I've seen that exhibits this behavior. Both
> Excel 4.0 and Excel 98. It gets worse. If you create a folder hierarchy on
> the floppy that mimics the hard drive, you can save files anywhere on the
> hard drive. It gets even worse. It lets you replace a file with the same
> name. It doesn't even prompt you with the "file already exists" dialog. For example, I just saved an Excel spreadsheet called Finder. I
> tried to save it in a folder called "System Folder" on an otherwise empty
> floppy disk called "Macintosh HD." It did exactly what you'd think it
> would do."

✶ Identity theft defeated by victim's wife

Jim Griffith <griffith@netcom.com>

Fri, 13 Nov 1998 15:48:20 -0800 (PST)

AP reports an unusual ending to an identity theft case. A man in North Carolina attempted to open a checking account at a BB&T branch

by presenting relevant information, including birthdate and Social Security number. One of the bank's tellers examined the paperwork, and she called the police after she realized that the information described her husband, who had died three weeks earlier. Police charged the suspect with two charges of obtaining property under false pretenses, and they are investigating how the suspect obtained the dead man's information and birth certificate.

🔥 Electronic Commerce: The Future of Fraud

Bruce Schneier <schneier@counterpane.com>

Fri, 13 Nov 1998 18:31:03 -0600

[This appeared in my November newsletter, CRYPTO-GRAM, <http://www.counterpane.com/crypto-gram.html>, but I thought it is of general enough interest to send it here.]

Electronic Commerce: The Future of Fraud

Fraud has been perpetrated against every commerce system man has ever invented, from gold coin to stock certificates to paper checks to credit cards. Electronic commerce systems will be no different; if that's where the money is, that's where the crime will be. The threats are exactly the same.

Most fraud against existing electronic commerce systems -- ATM machines, electronic check systems, stored value tokens -- has been low

tech. No matter how bad the cryptographic and computer security safeguards, most criminals bypass them entirely and focus on procedural problems, human oversight, and old-fashioned physical theft. Why attack subtle information security systems when you can just haul an ATM machine away in a truck?

This implies that new commerce systems don't have to be secure, but just better than what exists. Don't outrun the bear, just outrun the people you're with. Unfortunately, there are three features of electronic commerce that are likely to make fraud more devastating.

One, the ease of automation. The same automation that makes electronic commerce systems more efficient than paper systems also makes fraud more efficient. A particular fraud that might have taken a criminal ten minutes to execute on paper can be completed with a single keystroke, or automatically while he sleeps. Low-value frauds, that fell below the radar in paper systems, become dangerous in the electronic world. No one cares if it is possible to counterfeit nickels. However, if a criminal can mint electronic nickels, he might make a million dollars in a week. A pickpocketing technique that works once in ten thousand tries would starve a criminal on the streets, but he might get thirty successes a day on the net.

Two, the difficulty of isolating jurisdiction. The electronic world is a world without geography. A criminal doesn't have to be physically near a system he is defrauding; he can attack Citibank in New York from St.

Petersburg. He can jurisdiction shop, and launch his attacks from countries with poor criminal laws, inadequate police forces, and lax extradition treaties.

And three, the speed of propagation. News travels fast on the Internet. Counterfeiting paper money takes skill, equipment, and organization. If one or two or even a hundred people can do it, so what? It's a crime, but it won't affect the money supply. But if someone figures out how to defraud an electronic commerce system and posts a program on the Internet, a thousand people could have it in an hour, a hundred thousand in a week. This could easily bring down a currency. And only the first attacker needs skill; everyone else can just use software. "Click here to drop the deutsche mark."

Cryptography has the potential to make electronic commerce systems safer than paper systems, but not in the ways most people think. Encryption and digital signatures are important, but secure audit trails are even more important. Systems based on long-term relationships, like credit cards and checking accounts, are safer than anonymous systems like cash. But identity theft is so easy that systems based solely on identity are doomed.

Preventing crime in electronic commerce is important, but more important is to be able to detect it. We don't prevent crime in our society. We detect crime after the fact, gather enough evidence to convince a neutral third

party of the criminal's guilt, and hope that the punishment provides a back-channel of prevention. Electronic commerce systems should have the same goals. They should be able to detect that fraud has taken place and finger the guilty. And more important, they should be able to provide irrefutable evidence that can convict the guilty in court.

Perfect solutions are not required -- there are hundred of millions of dollars lost to credit card fraud every year -- but systems that can be broken completely are unacceptable. It's vital that attacks cannot be automated and reproduced without skill. Traditionally, fraud-prevention has been a game of catch-up. A commerce system is introduced, a particular type of fraud is discovered, and the system is patched. Money is made harder to counterfeit. Online credit card verification makes fraud harder. Checks are printed on special paper that makes them harder to alter. These patches reduce fraud for a while, until another attack is discovered. And the cycle continues.

The electronic world moves too fast for this cycle. A serious flaw in an electronic commerce system could bankrupt a company in days. Today's systems must anticipate future attacks. Any successful electronic commerce system is likely to remain in use for ten years or more. It must be able to withstand the future: smarter attackers, more computational power, and greater incentives to subvert a widespread system. There won't be time to upgrade them in the field.

[Note: Why Cryptography is Harder Than it Looks appeared in [RISKS-18.59](#),

and is also at <http://www.counterpane.com/whycrypto.html>]

Security Pitfalls in Cryptography: <http://www.counterpane.com/pitfalls.html>

Bruce Schneier, President, Counterpane Systems Phone: 612-823-1098

101 E Minnehaha Parkway, Minneapolis, MN 55419 Fax: 612-823-1590

Free crypto newsletter. See: <http://www.counterpane.com>

✶ Password capturing

Bill Carton <bill_carton@credence.com>

Thu, 12 Nov 1998 10:14:21 -0800

A new web site was featured on the 10 Nov 1998 morning TV spot, Bloomberg

Tech Report: www.thatweb.com. It purports to be a single site from which you

can download POP mail from your personal ISP, in case you're behind a

firewall at work, for instance.

It asks for your e-mail address and password, and in response to signing up,

spits out seven pages of legal boilerplate that says you agree to not use

their service to spam, harass, or other "illegal or immoral purposes". The

typos made me think it was not a native English-speaker who set this up, and

indeed, the Webmaster replied from Singapore. The site is not secure, of

course.

So why did Bloomberg's reporter feature this GAPING security hole? Unclear.

I wrote them:

```
> > From: bill_carton@credence.com
> > Sent: Thursday, November 12, 1998 7:04 AM
> > To: webmaster@thatweb.com
> > Subject: Privacy and Security
> >
> > Since you have the capability to capture and archive
> > individuals'
> > passwords, common sense requires you to provide a privacy and
> > security statement.
> >
> > I see none on your Web site. Please supply your potential
> > users with
> > something that can be verified by someone of an unimpeachable
> > reputation who is known by net security experts.
> >
> > Otherwise, your site seems indistinguishable from a login
> > screen
> > spoofer - and will only be used by clueless newbies. Is
> > that the
> > audience your advertisers want to be paying for? A very poor
> > demographic indeed.
> >
> > At the very least, it needs to be a secure site, but you
> > will have
> > to do a LOT more to gain the trust of the net community. Do
> > you
> > read comp.risks? You should.
> >
> > Bill Carton
```

Mun Hon Pheng - PO wrote:

```
>
> Dear Sir,
>
> Thank you for your suggestion. We are indeed working on
> making this site a
> secure site with the necessary protection for data privacy and
> security.
```

No, I believe you do not understand. Your Web site should not have been placed on the Web in its current condition. It MUST have been secure on Day #1. You cannot make it secure now, and have anyone trust it. Your reputation is already damaged, and you have no credibility with anyone who has been thinking deeply about security issues.

> Would appreciate it if you can recommend someone with unimpeachable
> reputation for knowledge of net security that we can consult regarding
> verification of our security procedure and set up.

Again, are you familiar with the usenet newsgroup comp.risks? You should have had someone on your staff already to answer these questions and prevent you from going public until they were adequately answered.

> We value your comments and suggestion. As we are incrementally improving
> our Web site, would appreciate your regular visit and follow up comments to
> help us improve.

My most basic comment is that this site should not be on the Web today. It is a serious security risk to anyone who is thoughtless enough to use it. E-mail security is a serious professional issue, and you have shown your disregard for those issues by your appearance on the net.

Please tell me what prevents you from keeping a file containing your user's e-mail addresses and passwords, and then downloading their mail for your own purposes? The public has NO ASSURANCE that you cannot or will

not steal
their mail, read their messages, and use any information you
discover for
your own purposes. Claiming you will not do these things is not
sufficient!
You are indistinguishable from thieves who might claim the
identical things.

The burden of proof is on *you* sirs, to prove your good
intentions, and
demonstrate you have taken proper precautions for data privacy
and
security. You should be familiar with an old trick, used for
decades at
computer centers at colleges. A program is left running on a
terminal, whose
entire appearance is identical to a login display. Then the
thief leaves the
room. A second user, the victim, then sits down and innocently
types in his
login name and password. The running program captures this
information,
e-mails it to the first person, and then exits. The victim
thinks his login
attempt has just failed, and tries again. This time it works OK.
But the
first person now has the victim's login name and password.

To a security-thinking individual (and there are thousands like
me) - you
have just created a Web-based version of this. It is up to YOU
to convince
US that it is not true. If you cannot, then we will do
everything possible
to educate your potential victims to avoid using your site.
These issues are
already being discussed on the usenet newsgroup news.admin.net-
abuse.email.

We await your reply at your earliest convenience.

Thank you, Bill Carton

Credence Systems Corporation, 9000 SW Nimbus Ave., Beaverton;
OR;97008
bill_carton@credence.com 1-503-350-7655

🔥 REVIEW: "Virus Alert of the Day", virus-alert@optimator.win.net

"Rob Slade" <rslade@sprint.ca>
Thu, 12 Nov 1998 09:45:53 -0800

MLVAOTD.RVW 981016

"Virus Alert of the Day", virus-alert@optimator.win.net, 1998,
<http://www.tipworld.com/changes.html>

%A virus-alert@optimator.win.net
%C City (place of publication)
%D 1998
%I TipWorld
%O <http://www.tipworld.com/changes.html>
%P 1 paragraph daily
%T "Virus Alert of the Day"

Aside from VirusHelp (cf. MLVIRHLP.RVW) and the rather noisy alt.comp.virus, there is one other regular source of virus information. No discussion, since this is a one way list, but one more source of clutter for your mailbox.

Virus Alert of the Day is one of the (very many) TipWorld mailing lists. Like all of them, it is primarily an advertising tool, so expect a lot of ads. In the case of the virus alert list, you can expect roughly a one paragraph tip per day, along with several screens of commercial announcements of various types. Actually, that is not quite true. There is usually about a screenful of viruses due to go off on the day in question. However, this is only a list of names,

without descriptions, and there are, of course, a great many viruses that can go off on any day, or are not subject to date alerts.

The information provided by this list is highly suspect. The author, and the closest I've been able to get to an identity is virus-alert@optimator.win.net, provides very little information, and does not betray much basic fact, let alone conceptual, checking in the postings. (Yes, doing it on a daily basis is hard, but remember that I ran the CVP postings for three solid years, week in and week out, and wasn't even close to running out of material.) Some comes from recycled press releases alerting users to new viruses or types. Sometimes the tip of the day is simply an announcement of a new antiviral release, ensuring that the entire message for the day is one long string of ads. But sometimes when the list actually tries to help it does the greatest disservice.

Let's look at three postings from the recent past. On September 10th, readers were advised to "Lock your floppies." Apparently, if you just "flip the `switch' up on the top-left corner on the back of the diskette ... you can prevent diskette-transferred viruses from being loaded onto your PC." Now, it's very nice that the instructions were that detailed, but, unfortunately, they were flat out wrong. If your computer is already infected, then locking your floppy disks may keep viruses off the floppy. But if your diskette is infected, locking it will do nothing to protect your computer. (This tip was later corrected by a reader.)

September 16th saw a note from a reader wondering what to do about an infection by a stealth, boot sector virus. He had tried various antivirals and none had removed it. The advice was to wait until the antiviral vendors got around to a release that did deal with it. Unfortunately, a number of the antivirals the reader had mentioned do deal with the virus, and quite effectively. The real secret in this case is to ensure that you "boot clean" and ensure that the virus is not resident in memory before you try to run the antiviral. The secret to booting clean is to ensure that your boot disk was created before the virus infected the system.

October 2nd saw the relaying of Symantec's report of the world's first Java virus. This viral non-event was widely ignored by the virus research community, since everyone had already known it was possible. Java is a computer language much like any other, and you can write anything you want in it. The potential threat of a Java virus lies in Java's ability to create applets for the Web. Fortunately for Web users, and unfortunately for "Strange Brew," applets submitted over the Web and run in browsers are confined to a "sandbox" that restricts some of the operations which "Strange Brew" needs in order to run.

On October 16th, users of Microsoft Word were told, in order to avoid spreading MS Word macro viruses, to save files in RTF (Rich Text Format) if they were going to send them to other users. Now, while this advice might be inconvenient (RTF is not capable of saving all possible MS Word

formatting information), there is some valid reasoning behind using it as a security precaution. RTF does not support MS Word macro viruses, either, so an RTF file wouldn't transmit them. A *true* RTF file, that is. A number of common macro viruses intercept the FileSaveAs call. CAP, for one, will save the file as a template document, with the infection present, in spite of the RTF extension on the filename.

Should you wish to chronicle the further misadventures of the virus alerts, check out the TipWorld signup page at <http://www.tipworld.com/changes.html>.

copyright Robert M. Slade, 1998 MLVAOTD.RVW 981016

⚡ REVIEW: "VirusHelp", Henri Delger

"Rob Slade" <rslade@sprint.ca>
Fri, 13 Nov 1998 11:22:02 -0800

MLVIRHLP.RVW 981011

"VirusHelp", Henri Delger, 1995,
http://goodstuff.prodigy.com/Mailing_Lists/virushelp.html

%A Henri Delger henri_delger@prodigy.com
%D 1995
%O <http://pages.prodigy.com/virushelp/vhelp.htm>
%P ~ 10 p. monthly
%T "VirusHelp"

VirusHelp does not predate the creation of the alt.comp.virus newsgroup, but with the current suspension of the VIRUS-L/comp.virus list it forms the oldest and most reliable ongoing interactive virus

information resource on the net. Moderated by Henri Delger, it is not something you can set your watch by, but you can generally expect at least two issues per month.

Each issue contains several questions or comments from readers, generally with answers or expansion from Mr. Delger. However, there are numerous leading antiviral experts who subscribe to the list as well, and who may write in with answers or information. Because of the moderation the quality of the discussion is very high, although traffic is relatively low.

In comparison to other virus lists and groups, many messages relate to the operation, strengths, and weaknesses of specific antiviral software. Other discussions include the usual calls for help when noticing some strange happening, as well as warnings about new viruses or trojans on the loose. Debate about potential, but not actual, new virus operations or concepts related to viral or antiviral technology is not unknown. Although the majority of messages are associated with Wintel systems other platforms are not excluded and messages about Macs, for example, are proportionately much higher than on other lists.

Generally the moderator will comment on all messages received, even those providing, or purporting to provide, information. Virus "experts" seem to grow under every bush, so Delger is quite free with correction when it is called for. He is free with opinion, but clearly indicates it as such.

Each issue also contains a large, if not exhaustive, list of recent antiviral software releases for a number of operating systems. The inventory specifies software, filename and release date, although the location of the file is left to the reader. (If you are a Prodigy subscriber, all of the listed files are available from a library there, and Delger does provide a list of vendor sites.) A recent addition has been a consistent warning against Internet hoaxes, particularly false virus alerts.

Subscriptions are free of charge, and may be obtained via the Web at:

<http://pages.prodigy.com/virushelp/vhelp.htm>

General virus information and back issues of VirusHelp are available

at <http://pages.prodigy.com/virushelp/> or the mirror at http://pages.prodigy.net/henri_delger/index.htm. Messages to the list

itself can be addressed to virushelp@listserv.prodigy.com.

copyright Robert M. Slade, 1998 MLVIRHLP.RVW 981011



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 9

Friday 27 November 1998

Contents

- [German stock exchange bond futures goof](#)
[Chris Brand](#)
- [Palo Alto 911 system crash](#)
[PGN](#)
- [Security risks delay online registration system](#)
[Chenxi Wang](#)
- [Internet speech is "on the record"](#)
[Martin Minow](#)
- [Organized mail theft in Seattle](#)
[Jon Becker](#)
- [Risks of being ostentatious when embezzling](#)
[Mich Kabay](#)
- [New Zealand: Pledge on destroyed net sites](#)
[Mich Kabay](#)
- [Frames security hole](#)
[Lindsay Marshall](#)
- [Internet Explorer 4.01 Son of Curatango cut-and-paste flaw](#)
[PGN](#)
- [100-year-old woman "too old to vote"](#)
[Michael Zastre](#)

- [Naming Swedish Names on the Internet](#)
[Martin Minow](#)
 - [REVIEW: "Cryptography and Network Security", William Stallings](#)
[Rob Slade](#)
 - [REVIEW: "Java Cryptography", Jonathan Knudsen](#)
[Rob Slade](#)
 - [DCCA-7 preliminary program](#)
[Mike Reiter](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ German stock exchange bond futures goof

Chris Brand <cbrand@west.raytheon.com>

Thu, 19 Nov 1998 16:36:14 -0800

From the Electronic Telegraph (<http://www.telegraph.co.uk:90>),
19 Nov 1998:

A junior trader cost his employers an estimated 10 million pounds yesterday after a training exercise went disastrously wrong and he ended up taking part in an 11.5-billion-pound transaction. The trader, who is believed to work for a German financial institution, pressed the wrong buttons on his computer and caused panic on dealing floors in the City. Screens flashed up with the news that someone wanted to sell 130,000 German bond futures contracts, worth in excess of \$11.5 billion. [...]

The German-based trader's employers are contractually obliged to carry out the transaction, and will be forced to buy futures contracts in the open marketplace to complete it. One banker said: "His employers must have extremely lax controls. A trade that size should have sent alarm

bells
ringing." [...]

German bond futures are now predominantly traded on Eurex, a German-based electronic exchange, on which traders say it is relatively easy to enter the dealing programme instead of the training simulation programme. [...]

Chris [also noted by Nathaniel Borenstein <nsb@si.umich.edu> and "Koblizek, Vaci" <Vaci-Koblizek@deshaw.com>. PGN]

⚡ Palo Alto 911 system crash

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

Mon, 23 Nov 98 8:48:56 PST

Palo Alto's 911 emergency system crashed on 11 Nov 1998 when the backup power supply (UPS with batteries) failed, but the phone calls were successfully switched over to the Santa Clara County center in San Jose within 45 seconds. In this case, the backup had a backup. However, the outage also knocked out the city's main police and fire department radio transmitters for about 45 minutes, the backup for which uses walkie-talkies.
[Source: *Palo Alto Daily News*, 12 Nov 1998, p.6, via Glenn Story]

⚡ Security risks delay online registration system

Chenxi Wang <cw2e@cs.virginia.edu>

Fri, 20 Nov 1998 09:30:36 -0500 (EST)

Reported on *The Cavalier Daily* (20 Nov 1998), officials at the University of Virginia decided to delay activating the online registration system because of security concerns associated with the NT operating system. This system will allow students to register for classes over the internet, and will serve in addition to the phone-based system now in use. Security problems with the online system, according to the article, involved malfunctioning features that allowed access to student information without a PIN and a Social Security Number.

Chenxi Wang

✶ Internet speech is "on the record"

Martin Minow <minow@apple.com>

Tue, 24 Nov 1998 22:30:08 -0800

The current issue of Salon Magazine <<http://www.salonmagazine.com/21st/>> has an interesting article on the permanence of the net by J.D. Lasica <mailto:jd@well.com>. titled "The Net Never Forgets." (This URL will direct you to the current article, but Salon archives its "back issues".) The content will probably not surprise Risks readers, but might be worth reading for the range of issues Lasica raises.

"Once, words were spoken and vanished like vapor in the air; newsprint

faded and turned to dust. Today, our pasts are becoming etched like a tattoo into our digital skins."

Martin Minow <minow@pobox.com>

P.S.: For at least 10 years, I've recommended "never post anything you don't want to see on your resume."

🔥 Organized mail theft in Seattle

Jon Becker <jondb@gis.net>

Wed, 25 Nov 1998 00:38:01 -0800

An Associated Press item reported on the compromise of the single master key being used for tens of thousands of streetside and apartment mailboxes in the Seattle area, and the massive theft of U.S. postal mail. A ring of at least bandits is suspected of nightly raids. Voting officials urged voters to go straight to post offices with their absentee ballots. [Source: Letterless in Seattle -- region struck by mail thieves, *USA Today*, 24 Nov 1998, www.usatoday.com; PGN Abstracting]

[I may never mail anything again. Jon]

[Another terrible example of the one-key-fits-all theory, which of course has its implications for the use of master keys and escrowed keys in cryptography and digital commerce. PGN]

✶ Risks of being ostentatious when embezzling

Mich Kabay <mkabay@compuserve.com>

Wed, 25 Nov 1998 07:49:36 -0500

In Gloucestershire, England, 32-year-old Martin Keys was convicted on 19 Nov 1998 of using data diddling to enter fraudulent orders for chocolate bars -- 500,000 pounds (~US\$830,000) worth. A co-conspirator would take possession of large loads of Mars Bars and other treats and return part of the profits to Keys. Keys lived far beyond his official means as a shift supervisor and fabricated a series of preposterous stories to account for why he was rich enough to drive a new Saab, travel to the Caribbean and purchased an expensive new home for his girlfriend.

M. E. Kabay, PhD, CISSP / Director of Education
ICSA, Inc. <<http://www.icsainc.net>>

[Also bad: Mars-ter Keys. He should have been named Mars-ton Keys. PGN]

✶ New Zealand: Pledge on destroyed net sites

Mich Kabay <mkabay@compuserve.com>

Sun, 22 Nov 1998 07:54:14 -0500

Follow-up on previous IHug story:

New Zealand Herald 20 Nov 1998

The Internet Group says most of the Web sites destroyed by a hacker this week will be restored by Monday. A director, Nick Wood, said only five

commercial customers had so far reported losing a complete site. Most customers had a back-up which they were reinstalling. Electronic commerce sites were on another server. The company, usually known as IHug, believes an Auckland man used a sub-program in a customer's site to access the homepages server, and deleted about a third of the files. About 4500 sites were affected.

⚡ Frames security hole

<Lindsay.Marshall@newcastle.ac.uk>
Fri, 20 Nov 1998 12:27:16 +0000 (GMT)

There is a description and demo of a security hole with frames in web browsers at <http://www.securexpert.com/framespoof/start.html> - there is a version that works without javascript enabled as well.

<http://catless.ncl.ac.uk/Lindsay>

⚡ Internet Explorer 4.01 Son of Curatango cut-and-paste flaw

"Peter G. Neumann" <neumann@csl.sri.com>
Fri, 27 Nov 98 10:33:11 PST

BugNet earlier reported the so-called Cuartango Hole in Internet Explorer 4.01 and Windows 98. Microsoft has now issued a security bulletin on a variant thereof that exists despite the earlier patch. In essence, the

cut-and-paste function bypass IE4 security. A new patch now exists.

[Source: An article by Bruce Brown in MSNBC, 23 Nov 1998:

<http://www.zdnet.com/zdnn/stories/news/0,4586,2168253,00.html>]

✶ 100-year-old woman "too old to vote"

Michael Zastre <zastre@csr.csc.UVic.CA>

Fri, 27 Nov 1998 11:13:14 -0800 (PST)

The Quebec '98 election Website reported on 27 Nov 1998 that several elderly residents in a Montreal nursing home are ineligible to vote in Monday's provincial election. One of these is a 100-year-old woman. The chief returning officer for the riding sees no reason why they can't vote, but he is prevented by law from giving the woman back her right.

<http://www.quebec98.cbc.ca/news/fullstory/F04.html> (link may go stale)

I would guess the problem is a Misinterpretation of Dates bug in the Electoral Office software, but there could be other reasons for the centenarian's plight. However, what is RISKY about this story is the part that existing legislation might play in exacerbating the fallout from MoD/Y2K related failures. It is one thing for a computer to remove the right-to-vote from the young at heart aged 100+, but quite another to have legislation that inadvertently **forbids** a bureaucrat to fix the resulting mess; a computer system creates a situation for which a piece of legislation

must be applied (e.g., withdrawing a citizen's civil right), but in a context never envisioned by lawmakers.

Mike Zastre <zastre@csr.uvic.ca>

[Note added in archive: This is incorrect. See [RISKS-20.10](#). PGN]

✶ Naming Swedish Names on the Internet

Martin Minow <minow@apple.com>

Thu, 26 Nov 1998 23:31:52 -0800

A recent [RISKS-20.05](#) article by Jacob Palme, archived at <<http://catless.ncl.ac.uk/Risks/20.05.html#subj12>> noted that a new Swedish law made it illegal to name an individual by name on the Internet. According to an article in the Swedish Newspaper Svenska Dagbladet's web page, people who name individuals without their permission need not fear prosecution. "I intend to take a liberal interpretation of the law and use some common sense" said the Data Inspectorate's chief, Ulf Wideback. ... "But, if someone posts personal information that is sensitive, we will act." he noted.

The Personal Information Law follows an EU directive that predates the Internet's recent growth. Ulf Wideback understands that people may believe that the law has strange consequences for Internet users.

Martin Minow, minow@pobox.com

🔥 REVIEW: "Cryptography and Network Security", William Stallings

"Rob Slade, dotting grandpa of Ryan and Trevor" <rslade@sprint.ca>

Mon, 23 Nov 1998 11:10:07 -0800

BKCRNTSC.RVW 981010

"Cryptography and Network Security", William Stallings, 1999,
0-13-869017-0

%A William Stallings ws@shore.net

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

%D 1999

%G 0-13-869017-0

%I Prentice Hall

%O +1-201-236-7139 fax: +1-201-236-7131 betsy_carey@prenhall.
com

%P 569 p.

%T "Cryptography and Network Security: Principles and Practice
2nd edition"

This book is intended to serve both as a textbook for an academic course of study, and as a self-study and reference guide for practicing professionals.

The material has been extended to emphasize encryption and its central position in network protection. The structure and flow have been reorganized with both classroom use and solo instruction in mind, and additional teaching material, such as additional problems, have been added.

Chapter one is an introduction to the topics to be covered. In a practical way it outlines the concerns involved in the phrase computer security, and the priorities occasioned by the networked nature of modern computing.

There is also an outline of the chapters and sequence in the

rest of the book. While the text does note that cryptographic techniques underlie most of current security technologies this is only done briefly. Examples in the major categories listed would help explain this primary position.

Part one deals with conventional, symmetric, encryption and the various methods of attacking it. Chapter two covers the historical substitution and transposition ciphers. Symmetric block ciphers are discussed in chapter three, illustrated by an explanation of DES (Data Encryption Standard). The additional conventional algorithms of triple DES, IDEA (International Data Encryption Algorithm), and RC5 are reviewed in chapter four. The use of conventional encryption for confidentiality is outlined in chapter five.

Part three looks at public-key encryption and hash functions. Chapter six introduces public-key encryption and its uses in confidentiality, authentication, and key management and exchange. Number theory is the basis of these modern algorithms, so some basic mathematical concepts are outlined in chapter seven. Digital signatures and message authentication is introduced in some detail in chapter eight. The algorithms themselves are explained in chapter nine, including MD5 (Message Digest algorithm), SHA (Secure Hash Algorithm), and others. Protocols using digital signatures are described in chapter ten.

Part three takes this background material and relates its use in security practice. Chapter eleven looks at authentication, concentrating on Kerberos

and X.509. The examples of e-mail security systems given in chapter twelve are PGP (Pretty Good Privacy) and S/MIME (Secure/Multipurpose Internet Mail Extension). Security provisions for the Internet Protocol (IP) itself are reviewed in chapter thirteen. Web security, in chapter fourteen, again concentrates on protocol level matters, but also discusses the SET (Secure Electronic Transaction) standard at the application level.

Part four outlines general system security. To the general public the primary concern of security is to deal with intruders and malicious software, so it may seem odd to the uninitiated to find that both of these subjects are lumped together in chapter fifteen. Chapter sixteen finishes off the book with a description of firewalls and the concept of trusted systems that they rely on.

Each chapter ends with a set of recommended readings and problems. Many chapters also have appendices giving additional details of specific topics related to the subject just discussed.

For the instructor, student, and professional, this work provides thorough coverage, clear explanations, and solid information.

copyright Robert M. Slade, 1998 BKCRNTSC.RVW 981010
rslade@vcn.bc.ca rslade@sprint.ca robertslade@usa.net
pl@canada.com

Find virus and book info at <http://www.victoria.tc.ca/techrev/rms.html>

⚡ REVIEW: "Java Cryptography", Jonathan Knudsen

"Rob Slade" <rslade@sprint.ca>
Tue, 17 Nov 1998 10:06:21 -0800

BKJAVCRP.RVW 981018

"Java Cryptography", Jonathan Knudsen, 1998, 1-56592-402-9,
U\$29.95/C\$42.95

%A Jonathan Knudsen

%C 103 Morris Street, Suite A, Sebastopol, CA 95472

%D 1998

%G 1-56592-402-9

%I O'Reilly & Associates, Inc.

%O U\$29.95/C\$42.95 800-998-9938 fax: 707-829-0104 nuts@ora.com

%P 372 p.

%T "Java Cryptography"

This book is intended to teach experienced Java programmers how to add cryptographic elements to their applications. The text is not intended to teach encryption algorithms, basic Java programming, or the overall Java security model: there are other books that fulfill those functions. There is one other limitation: much of the book relies on the Java Cryptography Extensions (JCE) which are only available to those in the United States and Canada (nudge, nudge, wink, wink).

Chapter one lists some fundamentals of encryption and the relationship to security. There are also a couple of programs right off the bat that will let you explore message digests, and encrypting and decrypting messages. The basics of confidentiality, authentication, and some major cryptographic algorithms are outlined in chapter two. The explanations are quite terse, but not out of line with the aim of the book. Java Security Architecture

(JCA) is explained in chapter three, along with a quick overview of the API

(Application Programming Interface) and SPI (Service Provider Interface).

Chapter four introduces Java's own pseudo-random number generator, plus

programming for key seeds from keyboard timing. Key management, in chapter

five, is somewhat weak. The APIs only deal with hierarchical key certification, but this may simply be an example of Knudsen dealing strictly

with the language, and leaving the concepts to others. I was, however,

bemused at some passages that may have suffered from a lack of copy editing:

for example, one section that seemed to confuse production of Message

Authentication Codes with working on Macintosh computers.

Authentication of

various types is covered quite well in chapter six. Chapter seven's guide

to encryption covers details not normally dealt with in cryptography texts

because it must handle all matters related to getting an encryption

algorithm to actually function in an application.

Chapter eight gives enough detail about signed applets to prove that they

are going to be browser specific for a while. Security provider programming

is covered in chapter nine, using the ElGamal algorithm as an example. A

sample application is created using an encrypted version of the talk utility

in chapter ten. An e-mail application is created in chapter eleven using th

provider previously generated in chapter nine. Chapter twelve closes off by

looking at security design for the system overall.

Appendices review BigInteger arithmetic in Java, the Base64 encoding scheme

(an option for converting binary objects to text characters for e-mailing), Java archive files, Javakey, and a quick reference for the Java cryptography classes as covered in the book.

Knudsen states that the book is written, as far as possible, without assuming any prior knowledge of cryptography. In this aim he succeeds rather well. The programmer with no background in encryption can still add a reasonable layer of security to his or her application. Those who study further, of course, will be able to ensure a higher level of protection and reliability.

copyright Robert M. Slade, 1998 BKJAVCRP.RVW 981018
rslade@vcn.bc.ca rslade@sprint.ca robertslade@usa.net
pl@canada.com

✶ DCCA-7 preliminary program

Mike Reiter <reiter@research.bell-labs.com>
Fri, 27 Nov 1998 11:02:38 -0500

Seventh IFIP International Working Conference on
Dependable Computing for Critical Applications (DCCA-
7)

The Fairmont Hotel
San Jose, California, USA
January 6-8, 1999

IFIP Working Group 10.4 on Dependable Computing and Fault
Tolerance + ...

[Abridged for RISKS. PGN] Early Registration deadline 6 Dec
1998.

Full info and online (secure) registration form is available at

<<http://www.conjelco.com/dcca/>> or from registration@sei.cmu.edu.

Wednesday January 6, 1999

9 am: Assessment of COTS Components

* The Taxonomy of Design Faults in COTS Microprocessors by Algirdas

Avizienis and Yutao He of UCLA, USA

* Assessment of COTS Microkernels by Fault Injection by J.-C. Fabre, F.

Salles, M. Rodriguez-Moreno, and J. Arlat of LAAS, France

11am: Coping with COTS

* Minimalist Recovery Techniques for Single Event Effects in Spaceborne

Microcontrollers by Douglas W. Caldwell and David A. Rennels of UCLA,

* Building Fault-Tolerant Hardware Clocks from COTS Components by

Christof Fetzner and Flaviu Cristian of UCSD, USA

2pm: Formal Methods

* A methodology for proving control systems with Lustre and PVS by S.

Bensalem, P. Caspi, C. Parent-Vigouroux, and C. Dumas, D. Pilaud,

VERIMAG, France

* Prototyping and Formal Requirement Validation of GPRS: A Mobile Data

Packet Radio Service for GSM by Luigi Logrippo, Laurent Andriantsiferana, and Brahim Ghrabi of University of Ottawa, Canada

* Formal Description and Validation for an Integrity Policy Supporting

Multiple Levels of Criticality by A. Fantechi, S. Gnesi, and L. Semini

of Universite di Firenze, Italy

4:30pm: Distributed Systems

* Proteus: A Flexible Infrastructure to Implement Adaptive Fault

Tolerance in AQUA by Chetan Sabnis, Michel Cukier, Jennifer Ren,

William H. Sanders, David E. Bakken, and David Karr of University of

Illinois and BBN, USA

* Improving Performance of Atomic Broadcast Protocols Using

the

Newsomger Technique by Shivakant Mishra and Sudha M.
Kuntur of
University of Wyoming, USA

Thursday January 7, 1999

9am: Time-Triggered Architecture

* The Transparent Implementation of Fault Tolerance in the
Time-Triggered Architecture by Hermann Kopetz and Dietmar
Millinger of
TU Vienna, Austria

* Formal Verification for Time-Triggered Clock
Synchronization by Holger
Pfeifer, Detlef Schwier, and Friedrich W. von Henke of
University of
Ulm, Germany

11am: Fault Tolerance and Safety

* PADRE: A Protocol For Asymmetric Duplex Redundancy by
Didier Essame,
Jean Arlat, and David Powell of LAAS, France

* Experimental Validation of High-Speed Fault-Tolerant
Systems Using
Physical Fault Injection by R.J. Martinez, P.J. Gil, G.
Martin, C.

Perez, and J.J. Serrano of the University and Politecnica
of Valencia,
Spain

2pm: Models of Partitioning for Integrated Modular Avionics

* A Model of Cooperative Noninterference for Integrated
Modular Avionics
by Ben L. Di Vito of ViGYAN/NASA Langley, USA

* Invariant Performance: A Statement of Task Isolation Useful
for
Embedded Application Integration by Matthew M. Wilding,
David S.

Hardin, and David A. Greve of Collins Commercial Avionics,
USA

* A Model of Non-Interference for Integrating Mixed-
Criticality Software
Components by Bruno Dutertre and Victoria Stavridou of SRI
International, USA

4:30pm: Dependability Evaluation

* Dependability Modeling and Evaluation of Phased Mission

Systems: a

DSPN Approach by Ivan Mura, Andrea Bondavalli, Xinyu Zang,
and Kishor

Trivedi of University of Pisa and CNUCE/CNR, Italy, and Duke
University, USA

* Dependability Evaluation using a Multi-Criteria Decision
Analysis

Procedure by Divya Prasad and John McDermid of the
University of York,
UK

Friday January 7, 1999

9am: Panel: Certification and Assessment of Critical Systems

11:30am: Probabilistic Guarantees

* Probabilistic Scheduling Guarantees for Fault-Tolerant Real-
Time

Systems by A. Burns, S. Punnekkat, L. Strigini and D. R.
Wright of the

University of York and City University, UK

* Fault Detection for Byzantine Quorum Systems by Evelyn
Pierce, Lorenzo

Alvisi, Dahlia Malkhi, and Michael Reiter of University of
Texas at

Austin, and Bell Laboratories, USA

Phone: 412-268-7388 (inquiries only)

Fax: 412-268-7401

E-Mail: registration@sei.cmu.edu

General Chair: Charles B. Weinstock, Software Engineering
Institute, USA

Program Chair: John Rushby, SRI International, 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 20: Issue 10

Thursday 3 December 1998

Contents

- [Dulles radar fails for half-hour](#)
[Doneel Edelson](#)
- [Pilots: Runway crossings a safety hazard](#)
[Doneel Edelson](#)
- [DoD falsified Y2K data but has "good feeling" about future](#)
[Edupage](#)
- [Virginia library removes software filters](#)
[Edupage](#)
- [How the rest of the world views Americans](#)
[Declan McCullagh](#)
- [False 911 calls traced to spliced cabling](#)
[Bryan O'Sullivan](#)
- [Immigration process on hold due to fingerprint data format](#)
[Deepak N](#)
- [Interesting bug in SecurID software](#)
[Drew Dean](#)
- [V-Mail -- or Virus Mail?](#)
[Jason Stokes](#)
- [PalmPilots voiding car locks in Europe](#)
[Brig C. McCoy](#)

- [Sony infrared controllers lock up certain Macintosh systems](#)
[Fred Condo](#)
 - [IR-outfitted Macs and Sony remote controls](#)
[T Byfield](#)
 - [Paranoia or Parannoyance?](#)
[Al Christians](#)
 - [Y2K inflation risk](#)
[Marion Moon](#)
 - [Risks of Internet keywords](#)
[Erann Gat](#)
 - [Re: Internet speech is "on the record"](#)
[Silas S. Brown](#)
[Scott E. Preece](#)
 - [Re: 100-year-old woman "too old to vote"](#)
[Bob Heuman](#)
 - [Re: REVIEW: "Java Cryptography", Jonathan Knudsen](#)
[Fred Long](#)
 - [FEmSys99: Call for Participation/Program](#)
[Axel Poigne](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Dulles radar fails for half-hour**

"Edelson, Doneel" <doneeledelson@aciins.com>

Tue, 24 Nov 1998 12:40:04 -0500

Radar failed for 31 minutes at the Washington D.C. area Dulles International Airport, leaving air traffic controllers unable to tell the exact locations of circling airliners. Controllers had no information on the altitude, airspeed or identification of about a dozen planes circling the airport.

[Source: AP item in *USA Today*, 24 Nov 1998; PGN Abstracting]

✈ Pilots: Runway crossings a safety hazard

"Edelson, Doneel" <doneeledelson@aciins.com>

Fri, 13 Nov 1998 12:57:48 -0500

In an effort to speed up landings and takeoffs, tight runway crossings are common. In May 1997, strong winds were sufficient to alter the timing enough to force the aborting of the takeoff of a British Airways 747 at Chicago's O'Hare Airport because of a United jet landing directly in its path. Fortunately, the BA plane was able to stop in time, blowing 6 tires, locking 12 brakes, and scaring the passengers. Beginning with a discussion of this case, an article in **USA Today**, 13 Nov 1998 [PGN Stark Abstracting] analyzes the issues involved at some length.

✈ DoD falsified Y2K data but has "good feeling" about future

Edupage Editors <edupage@franklin.oit.unc.edu>

Sun, 29 Nov 1998 13:46:13 -0500

A Department of Defense inspector-general report says that the Defense Special Weapons Agency never conducted required tests on three of five "mission critical" computer systems it had certified as Y2K-compliant. The military officer assigned to correct the agency's Year 2000 problems says he agrees with the report, but that the systems in question will be "100% in compliance" by April 1999: "I have a good feeling about Y2K in

this agency."

(*USA Today*, 27-29 Nov 1998; Edupage, 29 Nov 1998)

✶ Virginia library removes software filters

Edupage Editors <edupage@franklin.oit.unc.edu>

Thu, 03 Dec 1998 13:39:32 -0500

Responding to a federal court's ruling that the Loudoun County (VA.) library's use of software filters to screen out sexually explicit material on the Internet was unconstitutional (Edupage 24 Nov 98), the Library Board has removed filters from some of its computers and left them on others; adults will decide whether they want to use a computer with a filter or one without, and parents of minors will be asked to sign a statement specifying whether or not they want their child to have unfiltered Internet access. Library patron Becky Montcastle-Jones urged the library board to appeal the court's ruling, saying: "We have not had pornographic or salacious material in our library. Why, just because we have new technology to get to it very quickly, should we have any different policy? In the video section, you can't go in there and get a pornographic movie. Librarians throughout history have had to make choices about what will be in the library. That's not censorship -- that's choice." But board member Marc Leepson expressed the view of 6 out of the 8 board members: "I'm completely comfortable with the new policy. It's constitutional, and it still protects children."

(*The Washington Post*, 3 Dec 1998; Edupage, 3 December 1998)

✶ How the rest of the world views Americans

Declan McCullagh <declan@well.com>

Tue, 01 Dec 1998 15:39:10 -0500

> Another federal judge killed another Internet censorship law,
> in the
> American state of Virginia; lawmakers, in order to protect The
> Children(tm) from all that smut on the Net, had ordered public
> libraries
> to install software filters; scoffed the judge, what a crock
> -- the law is
> unconstitutional, get those filters off, right now; not only
> that but the
> filters he saw even blocked Web sites about the Quaker
> religion and Beanie
> Babies. A Philadelphia judge delayed Mr Clinton's
> unconstitutional Child
> Online Protection Act, a censorship law that requires Web
> sites to prove
> the age of those who log on before showing them any pictures
> or "material
> considered harmful to minors," whatever that is.
> [*Bangkok Post*, database technology section, 2 Dec 1998 --
> with attitude...]

[<http://www.well.com/~declan/politech/>]

[VA VA voom!]

✶ False 911 calls traced to spliced cabling

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

Wed, 2 Dec 1998 01:10:36 -0800 (PST)

San Francisco police and Pacific Bell have traced the source of over 120 false calls to the 911 emergency service during a 36-hour period. The problem manifested itself through several telephones in San Francisco's Mission district that called 9-1-1 repeatedly; when operators answered the calls, they heard only static. Apparently, a phone cable became wet at the point of a splice and shorted out intermittently, causing this rather odd problem.

⚡ Immigration process on hold due to fingerprint data format

<Deepak_N1@Verifone.Com>

Mon, 30 Nov 1998 18:03:29 -0800

I just received this from my lawyer.

> Earlier this week, the INS suspended the processing of all I-485s filed
> with the INS Service Centers and District Offices on or after April 1,
> 1998. A written announcement will be issued by INS Headquarters in the
> very near future. The reason for the processing suspension is an error by
> the outside INS CLAIMS contractor, EDS, which failed to deliver
> fingerprint data tapes to both the FBI and CIA in a format that could be
> read by these agencies. The INS has been working to resolve the problem
> with the FBI and the CIA. Apparently, the FBI has now completed all
> fingerprint checks for applications filed with the Service through the end
> of September, 1998, but the CIA is still working on cases

filed in April,
> 1998. It is not clear at this time how long the processing
suspension will
> last. Concurrently filed I-765s and I-131s are not affected by
the hold.

> The immediate impact of the I-485 processing suspension will
be on
> applications filed at the NSC where they are now ready to
close-out April,
> 1998 filings. The backlogs at the other Service Centers and
most District
> Offices are much longer. Additionally, close-outs for aging-
out cases
> filed on or after April 1, 1998, are also on hold.

🔥 Interesting bug in SecurID software

Drew Dean <ddean@CS.Princeton.EDU>

Mon, 30 Nov 1998 16:56:54 -0500

I have a SecurID card for my Princeton Computer Science
department account.
The setup is that an old Sun, running SunOS 4.1.4, is running
the SecurID
software; you telnet to it, authenticate, and then rlogin to
where you want
to go. While this setup isn't perfect, the router hooking these
machines to
the outside world is setup to prevent spoofing, and the local
network is
deemed to be under reasonable control.

A couple months ago, I logged in, and tried to rlogin to the
workstation on
my (former) desk. It said, "Not on system console." Funny, it
only says
that if you attempt to rlogin as root. I looked a little more
closely,

noticed a # prompt, and /usr/bin/id reported that I was UID 0. Hmm. I had logged in as myself, and gotten a root shell on the SecurID server! How bizarre.... The head system administrator also received a root shell after logging in as himself.

Further investigation yielded that our entries in /etc/passwd were of the form +<username>::::: i.e., to get our information from NIS. However, due to a pending network reconfiguration, the machine was temporarily not using NIS, and no ypbind was running. It appears that the SecurID software didn't check the return value, and used a default value of 0. (The SecurID software keeps a separate database for its authentication information.) This raises interesting questions about a denial of service attack escalating to a root compromise (for local users; you need a SecurID card to login with). I do not have the time or facilities handy to investigate further.

In Security Dynamics defense, this software is more than 3 years old, and hasn't been updated because it otherwise works fine. (I can't find any version numbers in it).

Security Dynamics has been notified.

Drew Dean <ddean@cs.princeton.edu>

V-Mail -- or Virus Mail?

Jason Stokes <jstok@SPAMBLOCKED.apana.org.au>

2 Dec 1998 10:53:32 GMT

Just read about a new voice mail over e-mail product from Philips, reported in "New Scientist" for 28th November.

Previous V-mail systems have worked only if the recipient has matching software to decode the sound-and-video file, but Philips

bundles matching playback software with the message and packages it

as a small executable file. The playback software works with any

version of Windows.

I don't have to remind comp.risks readers of the potential for viruses and

Trojan horses to spread after being inserted into executable files sent

over e-mail. Ugh.

Jason Stokes: jstok@bluedog.apana.org.au

[No, you don't, but apparently we need to remind everyone else. PGN]

⚡ PalmPilots voiding car locks in Europe

"Brig C. McCoy" <brigc@world.std.com>

Thu, 03 Dec 1998 16:34:45 -0600

There's at least one program for Palm devices with IR ports which "learns"

the infrared codes from a remote-control device, letting the Palm device

replace remote controls for your TV/VCR/Cable/Stereo/Whatever.

According to a story in *New Scientist*, this same program can

be used to
"learn" the codes from several different makes of remote locks
for cars in
Europe.

Wonder if 3Com's planning to include an RF interface for US
cars? :)

<<http://www.newscientist.com/cgi-bin/pageserver.cgi?/ns/981205/newsstory6.html>>

Brig C. McCoy, Southeast Kansas Library System, 218 East Madison
Street,
Iola, KS 66749 1-316-365-5136 <<http://www.sekls.lib.ks.us/staff/brigc>>

[The NS article says that it takes only 10 seconds to capture
the code,
and is virtually undetectable. Discovery is credited to Lars
Sorensen of
PC World. I recall mention of this attack mode in RISKS many
years ago.
(Watch out for palm-palm girls.) Also noted by several
others. PGN]

✶ Sony infrared controllers lock up certain Macintosh systems

Fred Condo <fcondo@csuchico.edu>
Wed, 2 Dec 1998 10:21:01 -0800

The Macintouch Web site reports at <<http://www.macintouch.com/time.html>> on
an interaction between Sony infrared remote controllers and
certain
Macintosh models with infrared receivers. A risk of adopting a
ubiquitous
control technology for unrelated machinery where commands may
leak between
systems.

✶ IR-outfitted Macs and Sony remote controls

t byfield <tbyfield@panix.com>

Wed, 2 Dec 1998 13:47:46 -0500

The 3 Dec 1998 Macintosh reports that wristwatches "capable of sending IR remote controls to common brands of televisions" can also, it seems, control some Macs outfitted with an IR receiver on the front of the box <<http://www.macintosh.com/time.html>>. Symptoms varied between models (various Performas and LCs) and OS revisions (7.5.5-8.1), and despite several standard problem-prevention/solution techniques, ranging from access/function-limiting software to disabling extensions at startup. Problems included crippling slowness (several-minute delays in responses to input), and the necessary fixes seem to be quite varied, up to requiring a full hardware reset.

The interesting thing is that these machines are doing exactly what they were designed for: respond to a Sony-compatible remote control. They could be powered up and down, the volume could be changed, and Apple Video Player could be launched with the TV/ Video button on the remote. Unfortunately, the remote--which in this case was a *wristwatch*--could send commands the machines couldn't cope with at all. Given the usual repertoire for solving enigmatic problems, it's a wonder that the sysops in the lab who stumbled across this problem actually figured it out--after running disk

utilities,
reinstalling software swapping hardware, and so on and so forth.
Obviously,
this trick could be the bane of innocent consumers who may have
bought a
particular Mac *because* it has some "multimedia integration"
capability--and a real boon to someone who wanted to hogtie a
computer lab,
staff and all.

What's especially noteworthy is the fact that this hardware/
software
integration can launch an application. Unless this is done by
some
completely nonstandard method, the MacOS does so *by name* --
which means
that if someone could contrive a way to install some relatively
powerful
software (e.g., UserLand Frontier) and rename it "Apple Video
Player," say,
while a sysop was off in search of some utility CD, s/he could
pretty much
have run of the house--without requiring direct physical access
to the
machine (a well-placed window would do just fine).

Ted

✶ Paranoia or Parannoyance?

Al Christians <achrist@easystreet.com>

Tue, 01 Dec 1998 00:59:46 -0800

A curious thing happened to me last week. I made, by telephone,
a hotel
reservation in a distant city. About 12 hours later, I received
by e-mail,
a commercial solicitation from an 'escort service' in the same
city. The
solicitation was sexually explicit and obviously aimed at those

who would
like to do business with prostitutes.

I did not give my e-mail address to the hotel, but I did make the reservation using my name exactly as I sign usenet postings, so I suspect that the hotel provided my name to someone who looked up my e-mail address in a compiled database and sent the solicitation.

This juxtaposition of events disturbs me, for the following reasons:

1. A presumably reputable business, the only kind with which I deal, is likely providing personal information about me to a disreputable one. If 'escort services' can obtain this information about me, what other doers of unseemly deeds might also obtain it?

2. Not only don't I know of any way to prevent such solicitations in specific instances, I don't know of any way to keep such marketing methods from proliferating into business-as-usual.

3. I have long held 'thou shalt not tempt' to be one of the major dictums of modern morality. The power to tempt is the power to corrupt and destroy.

4. A little paranoia, inspired by this surprising evidence that someone out there knows more about me than I want them to know, gets me thinking where this will lead. It is easy to imagine that a business obtaining customers this way might next go ahead and find out if the client has a spouse back home. They might then send mail or e-mail to the spouse or household that is intended to raise the spouse's suspicions of infidelity. The

might send solicitations to the spouse for detective services to check up on their itinerant mate. They might send solicitations to the spouse for similar 'escort services' while their mate is away. They might market legal services related to divorce to each spouse. That would all be legal. If they wanted to do anything illegal, the opportunities for extortion and blackmail abound.

5. Other vices and weaknesses might be exploited similarly. Travelers away from home are often separated from the social support that they may need to regulate their behavior. Customized mass-marketing like this could profitably target those with problems related to gambling, liquor, etc. According to my morality, it would be wrong to exploit the weaknesses of the weak when they are most vulnerable, but it seems inevitable that there will always be some who can't resist taking advantage and some who will tragically be their prey.

Al Christians

Y2K inflation risk

<mmoon@west.raytheon.com>

Mon, 30 Nov 1998 11:09 -0800 (PST)

Here is another unintended consequence of technology. When a local regional hospital could not get the vendor of an older *analog* nuclear medicine

machine to declare that the machine was Y2K compliant, the hospital decided to buy a new digital machine at a cost of over \$700,000. The older machine was still useful but the hospital felt it would be liable if it couldn't state that the machine was compliant. It is doing the same thing with other less expensive machines also -- discard and replace. The implications for patients and insurance companies is obvious; no wonder medical cost inflation is increasing faster the CPI.

Marion Moon

⚡ Risks of Internet keywords

Erann Gat <gat@binkley.jpl.nasa.gov>

Wed, 2 Dec 1998 13:21:56 -0800 (PST)

Internet keywords are a new feature in version 4 of Netscape Navigator. On the surface they seem like a great idea: instead of just a URL, you can now type a set of search keywords in the "location" selector mini-buffer at the top of the browser. Anything that is not a valid URL is interpreted as search keywords and are sent to Netscape's search engine. It seems like a cool feature that can save you a step when you are doing a search. Instead of having to go back to the search engine every time, you have a shortcut to a search engine always at the ready.

So just now I was editing some records in a web database on one of our local

servers when I was suddenly surprised by the appearance of a set of search results from the Netscape search engine. What's more, every attempt to get back to the database server resulted in the same set of search results. Even typing in the URL with the http:// header didn't help. It was as if the search engine had suddenly hijacked my browser. What's more, trying to access the server from a different browser running on a different machine yielded the same result!

What turned out to have happened is (I think) this: the database server suddenly shut down for reasons unknown. Because I had typed in the URL without the domain (since it was a local machine) Netscape now interpreted the name of the machine (which, as far as Netscape was concerned, had suddenly ceased to exist) as an internet keyword, which popped me in to the search engine.

A little sleuthing turned up an extra risk: before dumping me in to the search engine it turned out that Netscape tried several variations on the machine name, such as prepending 'www' onto the name. It turned out that none of these variations existed, but if they had I could have suddenly found myself looking at a completely random web page. If this page happened to have content deemed "inappropriate" for viewing at work I might have had a hard time explaining to Big Brother that I really had not intended to download that page.

What made it all the more confusing was this: the database

server was running on a nonstandard port, so the URL I originally typed looked like "server:81". Only the database server died, not the whole machine, so going to the URL "server" still did the Right Thing (i.e. it took me to the server's http home page). Only when qualified with a port number for a nonexistent service did this problem manifest itself. Netscape is apparently not smart enough to figure out that the existence of a port qualifier in the URL means that this is **not** a keyword. (Netscape does seem to know that a fully qualified host name with its domain name should not be interpreted as a keyword.)

There are several risks here: 1) An apparently useful feature displays surprising and potentially dangerous behavior. This surprising behavior can be triggered suddenly by a crash on a different machine. There is no indication as to the actual source of the problem. 2) The existence of internet keywords fills out the space of legal things to type in to the "location" buffer in the browser, making it more likely that a typo will take you somewhere you don't want to be rather than generating an error.

Erann Gat gat@jpl.nasa.gov

✉ Re: Internet speech is "on the record" (Minow, [RISKS-20.09](#))

"Silas S. Brown" <ssb22@cam.ac.uk>
Sat, 28 Nov 1998 06:42:35 +0000

The *Salon* article several times mentions searching for a person's name, the assumption apparently being that that is a unique identifier. It is not. For example, every so often my Web page gets hits with an AltaVista query for "Silas Brown" as the referral page, and I recently received fan mail destined for a Silas Brown who is apparently a religious pop singer in America (and doesn't seem to have an online presence). My name is unusual in my culture but this is not universally true.

If someone called Yuki Tadeka (random example) were running for President of the US, and I were a sleaze journalist and showed you "Yuki Tadeka's Home Page" as it was twenty years ago, even if you could prove by going to the archives yourself that the page really existed, how would you know that it was generated by the same person?

Somewhere on www.newscientist.com is a rather misinformed letter written on 27 April 1996 by a "Silas S. Brown" about the nature of time and space (and they accidentally included the e-mail signature). If I denied that that was me, would you be able to prove otherwise?

Silas S Brown, St John's College Cambridge UK <http://ban.joh.cam.ac.uk/~ssb22/>
Databus magazine <http://www.cam.ac.uk/CambUniv/Societies/cucs/>

✶ **Re: Internet speech is "on the record" (Minow, [RISKS-20.09](#))**

Scott E. Preece <preece@urbana.css.mot.com>

01 Dec 1998 09:08:49 -0600

While the Web does sometimes seem to be all things to all people, it's ironic that while Martin Minow ([RISKS-20.09](#)) points at an article reminding us that web materials may persist far longer than we expect, archivists and librarians have decried the web as having no past, pointing out that today's link may tomorrow point into a cyber-hole and that the things that links point to may change unpredictably, so that that citations become meaningless. The web needs a Library of Congress-grade authoritative repository; it wouldn't hurt if there were also a reliable expiration mechanism...

scott preece, motorola/css urbana design center preece@urbana.
css.mot.com
1101 e. university, urbana, IL 61801 1-217-384-8589

⚡ Re: 100-year-old woman "too old to vote" ([RISKS-20.09](#))

<rsh@idirect.com>

Sat, 28 Nov 1998 11:23:50 -0500

Having read the information in my newspaper, it appears that age is **not** the reason for the removal of the right to vote, but rather a judgement that the little old lady is no longer completely competent. Note that three other residents of the same senior's residence were also denied the right to vote, and they were not yet 100 years old. They were interviewed in person,

and apparently her nodding of her head in response to questions was not deemed sufficient evidence of her competency. Whether this decision is correct or not is not subject to correction under the law being used - that is the real issue. It has nothing to do with computers or the two-digit/three-digit controversies.

R.S. (Bob) Heuman, Toronto, ON, Canada
<heuman@intria.com> or <rsh@idirect.com>

[Also noted by quite a few others. TNX. PGN]

Re: REVIEW: "Java Cryptography", Jonathan Knudsen (Slade, RISKS-20.09)

"Fred Long" <fwl@aber.ac.uk>
Mon, 30 Nov 1998 13:38:32 +0000

I really must take exception to Rob Slade, in his otherwise fine review of "Java Cryptography" by Jonathan Knudsen, where he says:

There is one other limitation: much of the book relies on the Java Cryptography Extensions (JCE) which are only available to those in the United States and Canada (nudge, nudge, wink, wink).

Firstly, the JCE is a **specification**, which is available world-wide.

Secondly, there are implementations of the JCE available outside the US and Canada as, indeed, the "Java Cryptography" book itself indicates. (Another book, "Java Security" by Scott Oaks, lists such implementations in an appendix.)

Dr Fred Long, Department of Computer Science, University of
Wales, Penglais,
Aberystwyth, SY23 3DB, UK +44 1970 622440 fwl@aber.ac.uk

⚡ FEmSys99: Call for Participation/Program

Axel Poigne <ap@borneo.gmd.de>

Thu, 3 Dec 1998 08:33:37 +0100

Workshop on Formal Design of Safety Critical Embedded Systems
15-17 March 1999, Munich, Germany

The workshop intends to bring together researcher, R&D engineers
from
industry, and tool vendors concerned with the specification and
construction
of Embedded Systems, particularly of Safety Critical Embedded
Systems.

For detailed information see

<http://set.gmd.de/EES/femsys99>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 11

Tuesday 8 December 1998

Contents

- [San Francisco power outage delays this issue](#)
[PGN](#)
- [How a FUSE caused a hospital to disconnect from the Power Grid](#)
[Joan L. Grove Brewer](#)
- [FAA investigating near-collision of passenger jets off Long Island](#)
[Richard Schroepel](#)
- [Y2K panic could be as disruptive as computer problems](#)
[Declan McCullagh](#)
- [NRC ERDS TMI risk?](#)
[Lloyd Wood](#)
- [MS Outlook's calendar shifts with time zone](#)
[Greg Marriott](#)
- [Shanghai entrepreneur tried in China](#)
[Edupage](#)
- [Typo causes wild stock fluctuations for wrong company](#)
[Lee Somerman](#)
- [Wassenaar Arrangement signed](#)
[Seth David Schoen](#)
- ["A very interesting development": export exemptions for free software](#)
[Seth David Schoen](#)

- [Electronic Vote Rigging? Shurely shome mishtake...](#)
[Malcolm Pack](#)
 - [Spamming to Spy](#)
[Dick Mills](#)
 - [Re: Dulles radar fails for half-hour](#)
[Steve Peterson](#)
 - [Re: the Internet has {no|perfect} memory](#)
[Mike Perry](#)
 - [A risk --or at least a highly undesirable use-- of JavaScript](#)
[Joe Thompson](#)
 - [Faulty failure modes](#)
[Mike Ellims](#)
 - [Re: Root login on SecureID server](#)
[Jay R. Ashworth](#)
 - [Author response to Slade review of Democracy & Technology](#)
[Richard Sclove](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **San Francisco power outage delays this issue (PGN)**

Neumann@CSL.sri.com <"Peter G. Neumann">

Tue, 8 Dec 1998 11:33:12 -0800 (PST)

At 8:15 this morning, failure of a power substation in San Mateo County south of San Francisco propagated, knocking two power plants off line, and affecting about 372,000 customers in San Francisco and some northern Peninsula cities, some for up to two or three hours. The blackout took down the SFO Airport, the Pacific Stock Exchange, rapid transit, and ATMs, as well as homes, offices, and hospitals. There were reports of people stuck in elevators and problems with home medical equipment. SFO was back up by

9:45 with emergency generators. The surge was felt in the North Bay and East Bay as well. SRI experienced only a power blip, but it was enough to wipe out a bunch of servers throughout the institute; CSL's computers were down for more than two hours. [Sources: patched together from various early on-line reports...]

[I look on this as a further reminder of how dependent we are on electric power, and how outages tend to propagate. Y2K-ologists will undoubtedly take this as a microcosm of what might happen on 1/1/00.]

⚡ How a FUSE caused a hospital to disconnect from the Power Grid:-)

"Joan L. Grove Brewer" <pegasus@transport.com>

Sun, 6 Dec 1998 15:29:29 -0800

In April 1998, the Valley Medical Center in Renton WA attempted to cut over to its new power cogeneration plant, independent of the local utility's power grid. The staff was apparently not adequately prepared, because it was assumed the cutover would be seamless. Initially, the hospital indeed ran smoothly, but then lights began to flicker, ventilation fans cut out, alarms beeped, and computer screens blinked on and off.

[Source: How a \$5.9

million power plant brought a hospital to its knees, by Byron Acohido,

Seattle Times staff reporter, *The Seattle Times*, 6 Dec 1998,

http://www.seattletimes.com/news/local/html98/vall_120698.html;

PGN Abstracting]

✶ FAA investigating near-collision of passenger jets off Long Island

Richard Schroepel <rcs@VISI.NET>

Tue, 8 Dec 1998 09:13:50 -0500 (EST)

A near collision between two Europe-bound passenger jets (British Caledonia L-1011 and Delta 767) occurred on the evening of 6 Dec 1998, avoided by onboard collision warning systems. Controllers blamed the absence on the expected earlier (2.5 minutes) warning from controllers on the failure of the Boston air-traffic control center in Nashua NH; the FAA is investigating. Over the same weekend, the FAA blamed onboard TCAS systems for a near collision over Albany NY. [Sources: *San Francisco Chronicle* 8 Dec 1998, A3 unourced, and an AP item from Boston, 8 Dec 1998, <http://www.nandotimes.com>; PGN Abstracting]

✶ Y2K panic could be as disruptive as computer problems

Declan McCullagh <declan@well.com>

Fri, 04 Dec 1998 12:36:38 -0500

One of the more interesting -- and perhaps serious -- Y2K risks is not computer snafus, but widespread panic. As Y2K coverage becomes increasingly mainstream (60 Minutes and CBS News ran pieces this week), stockpiling by individuals and businesses could lead to a recession or even

bank runs. At least that was the verdict at a Y2K summit on Thursday. --Declan

<http://www.wired.com/news/news/business/story/16618.html>

Bankers: Prepared for a Panic? 4:50 p.m. 3.Dec.98.PST
by Declan McCullagh (declan@well.com)

Fear of electric-power outages and bank failures could lead to widespread

panic as disruptive as the Y2K glitch itself, Senator Robert Bennett warned

Thursday at the first summit organized by President Clinton's Y2K council.

"Even if the Y2K problem is solved, the panic side of it can end up hurting

us as badly," said Bennett, the Utah Republican who heads the Senate's Year

2000 committee. [remainder snipped]

⚡ NRC ERDS TMI risk?

Lloyd Wood <L.Wood@surrey.ac.uk>

Fri, 4 Dec 1998 12:56:19 +0000 (GMT)

From: <http://xent.ics.uci.edu/FoRK-archive/nov98/0071.html>

[Ob-Bits] I recently discovered something interesting about the NRC's

(Nuclear Regulatory Comm.) ERDS (Emergency Response Data System). Instituted as a response to TMI (Three Mile Island) ERDS is the computer

link that US nuclear plants are supposed to use to transmit critical release

data in the event of an accident. Well, guess what, they have ONE modem at

the NRC. A big help that will be on Jan 1, 2000. Sleep tight.

[No URL

available, this is my own observation]

<L.Wood@surrey.ac.uk>PGP<<http://www.ee.surrey.ac.uk/Personal/L.Wood/>>

⚡ MS Outlook's calendar shifts with time zone

Greg Marriott <greg@spies.com>
Sat, 5 Dec 1998 14:41:47 -0800

Martin Minow <minow@pobox.com> suggested that I send this item.

A friend told me about this a few weeks ago. I didn't believe him. I had to see it for myself.

Just imagine... [wavy dream lines]

You live in San Francisco and go to New York for business. You enter all your business meetings in MS Outlook's calendar on your Windows laptop before you leave. You fly to New York and adjust your location (time zone) so your computer will what time it is. Then you miss a crucial appointment because the calendar claims a meeting is at 3pm even though you said it was at noon.

All your appointments get time shifted when you change your location. They claim this is a feature. I kid you not.

I can only guess that somebody decided appointments should be stored as GMT and then displayed as local times depending on the time zone the computer thinks it's in.

As to why they thought this was a good thing, I have no clue.

Greg Marriott

✶ Shanghai entrepreneur tried in China (Edupage)

Edupage Editors <edupage@franklin.oit.unc.edu>

Sun, 06 Dec 1998 13:36:36 -0500

The Chinese government has put 30-year-old Shanghai computer software businessman Lin Hai on trial for "inciting the overthrow of state power" by providing 30,000 e-mail addresses to a U.S. Internet magazine called "Big Reference" published by Chinese dissidents. Chinese authorities closed the four-hour trial for what it said were "national security" reasons, and "persuaded" one member of Lin's legal team not to attend the trial. Lin's wife Xu Hong, who was questioned by the police for six hours, has indicated that Lin's lawyer "said he didn't have a very good feeling -- that things won't be good for Lin and he will probably be found guilty." (*The Washington Post*, 5 Dec 1998; Edupage, 6 December 1998)

✶ Typo causes wild stock fluctuations for wrong company

"Lee Somerman" <lee@lmsconsulting.com>

Fri, 4 Dec 1998 20:29:42 -0800

That's Ticketmaster, With an 'S'
Wired News Report, 3 Dec 1998

Ticketmaster Online-CitySearch's initial public offering later today will raise a whopping US\$98 million for the online entertainment guide. It also bolstered the fortunes of a tiny office cleaning company in Manhattan, thanks to a misprint. Ticketmaster's stock is slated to trade under the symbol TMCS. But Reuters and ZDNet mistakenly printed the symbol as TMC0 in their coverage of the IPO.

TMC0 is the stock symbol of Temco Service Industries International. Because of the erroneous reports, the stock zoomed to an all-time high of \$65 from \$23. In early afternoon trading, the stock settled back down at \$31, after investors apparently figured out their mistake.

Representatives of the company were not immediately available for comment, nor were Ticketmaster officials.

Talk about a random walk on Wall Street.

Wassenaar Arrangement signed

Seth David Schoen <schoen@uclink4.Berkeley.EDU>
Fri, 4 Dec 1998 13:15:01 -0800

According to a press release and Reuters reporting, the Wassenaar Arrangement, a major treaty on export controls, has been signed by 33 member states. The most significant provision of the Arrangement from the point of view of most computer users is a promise by signatories to adopt US-style export controls on cryptography.

While the Arrangement does not dictate specific policies for its member states, they are still expected to try to bring their export rules in line with certain standards, which analysts said were dictated by the US and intended to promote an anti-crypto agenda.

The member countries are Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Republic of Korea, Luxembourg, The Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Russia, Slovakia, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom, United States.

Some of these countries are presently the major sources for the international distribution of cryptographic software.

<http://biz.yahoo.com/rf/981203/31.html>

<http://www.wassenaar.org/>

✶ "A very interesting development": export exemptions for free software

Seth David Schoen <schoen@uclink4.Berkeley.EDU>

Fri, 4 Dec 1998 14:15:13 -0800

According to some international developers of crypto software, some Wassenaar countries have exemptions in the works for free or Open Source crypto software (with various definitions of what's allowed). There are also supposed to be exemptions for public domain software.

The Norwegian developer Eivind Eklund wrote on slashdot.org:

I just got information on how Norway (where I live) implement this (ie, how the regulations are changed). The new rules prohibit export of crypto-software, but with a deliberate exception for open source software. This is a very interesting development.

Several other countries seem to be developing similar policies (including Sweden and Canada); these rules could protect the development of free crypto software on the Internet.

Seth David Schoen L&S '01 (undeclared) / schoen@uclink4.berkeley.edu

⚡ Electronic Vote Rigging? Shurely shome mishtake...

Malcolm Pack <mpack@email.com>

Fri, 04 Dec 1998 06:00:45 GMT

I recently received the following e-mail from a former colleague:

> An attempt is being made to influence the result of the voting for BBC Sports Personality of the year. It has been decided that David Beckham would provide most embarrassment to the organisers if winning, so could you all e-mail your vote to the following address:
>
> <sports.review@bbc.co.uk>
>
> More importantly, can you forward this mail to all your mates & acquaintances ASAP in the hope that they will participate.
>
> Your co-operation in this matter is greatly appreciated.

For those with no interest in English sport, David Beckham was the player who, by deliberately fouling another player during the recent Football (Soccer) World Cup in France, made himself responsible (the scapegoat?) for England's departure from the competition. To have to proclaim him "Sports Personality of the Year" would indeed be a delicious and embarrassing irony for the BBC.

<<http://www.bbc.co.uk/info/news/news132.htm>>

The intent of the mail is relatively harmless, even amusing. The risks to the BBC of opening up the voting to such an inexpensive, anarchic, insecure and easily-spoofed medium as e-mail are, as we so often have to say, obvious.

Needless to say, I've already registered my vote. ;-)

Malc, Southend-on-Sea, UK

Spamming to Spy

Dick Mills <dmills@albany.net>
Sat, 12 Dec 1998 20:54:32 -0500

In [RISKS-20.10](#), <jstok@SPAMBLOCKED.apana.org.au> (Jason Stokes) wrote about voice mail with embedded audio playback software embedded in e-mail. He said:

>I don't have to remind comp.risks readers of the potential for viruses and

>Trojan horses to spread after being inserted into executable files sent
>over e-mail. Ugh.

The post prompted me to think of the reverse kind of Trojan horse. If users accepted e-mail with embedded programs, and also leave their audio systems and or video systems enabled, then someone could send a mail message that would launch a program that would turn on the microphone and camera and transmit the information back to a remote location. Bugging via spam.

Hmmm, I wonder if there's an Internet enabled PC in the Oval Office or in the corridor outside?

Dick Mills <http://www.albany.net/~dmills>

✶ Re: Dulles radar fails for half-hour ([RISKS-20.10](#))

Steve Peterson <speterson@virtation.com>
Mon, 07 Dec 1998 22:56:45 -0600

[RISKS-20.10](#) reports that, due to a radar failure, "controllers had no information on the altitude, airspeed or identification of about a dozen planes circling the airport."

While radar failures are certainly important, it's wrong to say that radar failures deprive controllers of this information. In this situation, pilots report all three items (plus their position) to ATC via radio. ATC procedures provide for increased separation between aircraft to

compensate
for the lack of radar data.

In the US (and presumably elsewhere), there are many places where reports by the pilot are the only source of information on the location of aircraft.

Steve Peterson, Principal Consultant, Virtation Technologies, Inc.

<http://virtation.com> +1 612 948 9729

⚡ Re: the Internet has {no|perfect} memory ([RISKS-20.09-10](#))

<Mike_Perry@DGE.ceo.dg.com>

Fri, 4 Dec 1998 21:39:06 est

Before the last election here in the UK, the Labour party was against controls on encryption, and promised, on their website, to oppose them.

Now that they are in power, they are planning to introduce a law controlling encryption - all the usual key escrow, TTP stuff.

And they've quietly removed the pages on their site which promised opposition to such legislation.

Old fashioned paper pamphlets are impossible to retract, but I personally find the ease with which the Internet facilitates this Orwellian rewriting of history a bit scary.

The RISK? - not simple disappearance, but the replacement of the real past with a false one.

Mike Perry <mike_perry@dge.ceo.dg.com>

✦ A risk (or at least a highly undesirable use) of JavaScript

Joe Thompson <joe@orion-com.com>

Fri, 04 Dec 1998 12:44:42 -0500

Today I was browsing the Macintouch web site (<http://www.macintouch.com/>)

and saw a link to a Wired News article on Virginia's new proposal for

anti-spam legislation. As a Virginia resident and anti-spam activist,

wanting to know more from having seen bits yesterday, I clicked the link and got the article at:

<http://www.wired.com/news/news/politics/story/16591.html>

After reading the article I hit the Back button to go back and finish

today's Macintouch news. What happened next surprised me: a new browser

opened up and presented me with a survey, unasked-for and certainly unwanted.

Checking through the HTML code of the Wired article, I found the following

lines:

```
[...]
```

```
var MBIstudyUrl = "http://mass.mbinteractive.com/mass/bedemir.dll/"; //this
```

```
line will change for final deployment of pages.
```

```
[...]
```

```
function RDABV(){
```

```
[...]
```

```
    if(MBIsampledUser && MBIvisitor)
```

```
    {
```

```
        getSetMBICookie(MBICookName);
```

```
        if (MBICookie == "") MBICookie=0;
```

```
        window.open(MBIstudyUrl + MBIstudyName + "?Ntc=" +
MBIcellVal +
"&Ntookcook=" + MBIcookie , "survey");
        sampledUser = 0;
    }
[...]
```

```
[...]
```

```
<body bgcolor="#FFFFFF" text="#000000" link="#333399"
vlink="#660066"
alink="#666699" onUnload="RDABV()">
[...]
```

For those not familiar with JavaScript, "onUnload" is called whenever a page ceases to be displayed (the users types in a new URL, clicks a link, or clicks a navigational button on the toolbar). In this case, when I leave the Wired site, a URL is constructed from previously set variables and I am sent to it.

The security and privacy implications of a web page redirecting users to random sites without their prior knowledge or approval are obvious. A simple case is a web site which redirects the user to a pornographic site, triggering alarms in corporate monitoring software. -- Joe

Joe Thompson, Charlottesville, VA joe@orion-com.com
<http://kensey.home.mindspring.com/>

Faulty failure modes

Mike Ellims <mike.ellims@pitechnology.com>
Fri, 4 Dec 1998 17:55:02 -0000

Faulty Failure Modes or It could give you a heart attack.

A couple of nights ago I was talking on the phone to my father (who lives in Lower Hutt, New Zealand) from here in Cambridge, England when the line went dead. When I tried to ring back all I could get was a ringing tone. Now as my father had a quad heart bypass operation about four months ago and as far I could tell (even after ringing British Telecom) that the phone was working, I rang the police in Lower Hutt and asked to send a car around to check. They also attempted to phone and on getting no answer decided to upgrade the call to 111 (i.e. 911 in the US) and dispatched both a police car and an ambulance. My rather amused (and healthy) father was greeted by two emergency vehicles arriving on his doorstep as was an abused telephone "engineer" who had cut the wire carrying our conversation. The failure mode is of course that cutting a connection completely make it look as if someone won't or more importantly can't answer the phone. All was well though, as one of the police officers and one of the ambulance crew had been coached by father at football (soccer in US)... It's a very small world.

Mike Ellims Pi Technology <mike.ellims@pитеchnology.com>
www.pитеchnology.com +44 (0)1223 441 434

⚡ Re: Root login on SecureID server (Dean, [RISKS-20.10](#))

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

Sat, 05 Dec 1998 14:26:40 -0500

No, this one's not Security Dynamics' fault, as you've no doubt found out by now. This is a common, and well documented, failure of the NIS client code for most versions of Unix. The format of the "send other inquiries to the NIS server" line in your password file is such that, if NIS isn't running, you're likely to find yourself logged in as root, unless the administrator was careful.

I don't remember exactly, it may not be possible to avoid the hole at all and still have NIS run correctly when it `_is_` running; this is in the Red book, but I haven't read it lately, and it's not handy.

✶ Author response to Slade review of Democracy & Technology

Richard Sclove <resclove@amherst.edu>

Wed, 18 Nov 1998 10:27:57 -0500 (EST)

Response by Richard Sclove to Rob Slade review of `_Democracy and Technology_` in RISKS FORUM (6 November 1998 Volume 20 : Issue 05)

Several fans of my book, `_Democracy and Technology_` (New York and London: Guilford Press, 1995), urged me to reply to Rob Slade's recent review (RISKS FORUM 6 Nov. 1998). I thank Rob for taking the trouble to read my book. It's difficult to respond point by point to his criticisms, because in some instances these are matters of judgement, and who would be surprised if an

author disagrees with a negative review? But I'll do what I can within a limited amount of space.

Rob's principal, repeated complaint is that my empirical examples are unconvincing and too few in number, and that I provide no evidence that a democratic politics of technology can actually come about. I'm surprised, because numerous previous reviewers have found my book's rich array of empirical cases, and its careful balance of idealism tempered by realism, precisely its greatest virtue. One example: Professor Bart Schultz (University of Chicago), reviewing Democracy and Technology in the journal Ethics (Jan. 1997), judges that:

"The great strength of [Sclove's] book is surely in just this effort to bring together materials from the United States and across the globe, demonstrating how technology can and should be democratized. ... The Amish, the Berger Inquiry over the MacKenzie Valley Pipeline (in Canada), different policy strategies toward AIDS, the Dutch science shops and Denmark's consensus conferences, the Boimondau watchcase factory, the Mondragon system, the movement by people with physical disabilities for barrier-free design, the mobilization against toxic waste by the residents of Woburn, Massachusetts, the Chicago Center for Neighborhood Technology, Lucien Kroll's 'Zone Sociale' for the Catholic University of Louvain Medical School -- these are but a few of the cases marshalled to show how realistic it is to go beyond conventional economic analysis and unregulated

markets to make technological development subject to democratic design and assessment."

Rob Slade judges the provisional democratic design criteria that I propose without merit. His test case is that he finds that military technologies come up looking democratic using these criteria. His finding is perplexing. The first criterion I propose recommends avoiding technologies that support authoritarian social relations, and other criteria prescribe avoiding technologies that hinder democratic deliberation or that promote unduly centralized political power relations. Now, as my book also observes (on pp. 22, 232-233), nuclear weapons are associated domestically with highly centralized, secretive power relations that even circumvent the basic U.S. constitutional balance of powers (i.e., by allowing the President to put hundreds of millions of lives at stake without consulting Congress). On these grounds, I would judge, contrary to Rob, that nuclear weapons fail spectacularly to pass muster against the democratic criteria I propose.

A major motivation of my book is to establish the mildly audacious claim that democratic evaluation should supersede conventional economic analysis as the principal basis for technological decisions. (E.g., when fundamental democratic principles are at stake -- as I show they often are in technological decisions -- we shouldn't rely in the first instance on a narrow economic cost-benefit analysis.) Rob's review complains, however, that, "Economic theory is not actually challenged in chapter ten

[of Sclove's book]. Instead it is turned into a straw-philosophy. ..." Gosh, Rob, isn't it peculiar that trained economists don't seem to read my book that way at all? For instance, economics professor Steve Cohn writes in the Ecological Economics Bulletin (4th Quarter 1997):

"For economists, the meat of Sclove's theoretical argument is contained in Chapter 10, where he challenges the optimality conclusions conferred on market outcomes by neoclassical economics. ... The book is well worth reading and could easily contribute to courses in economics, political science, science and technology, and public policy."

Thus here and elsewhere, I find Rob's somewhat ranting style cute and engaging to read, but also judgementally sloppy, cavalier, and misleading.

On the other hand, I think a weakness in my book (albeit one that neither Rob nor other reviewers have noted) is that I didn't suggest a specific institutional means for debating and applying my provisional democratic design criteria within participatory settings. I'm currently working on that task under a grant awarded by the U.S. National Science Foundation and in collaboration with the Danish Parliament's Board of Technology. Indeed, my book is not at all a work in idle scholarship. The nonprofit Loka Institute, which I founded over a decade ago, works full-time on trying to promote a democratic politics of technology in practice, and we've had some notable successes (e.g., in promoting a worldwide network of

centers for
conducting community-based research, and in our introduction
into the
U.S. of European-style deliberative citizens' panels on science
and
technology policy). Anyone interested can learn more from
Loka's Web page
<www.loka.org> or by subscribing to Loka Alerts, our free,
occasional (and
quite popular -- 15,000+ subscribers worldwide) newsletter; just
E-mail a
subscription request to <Loka@amherst.edu>.

Stylistically and in the complexity of its argument, my book is
pitched
midway between a scholarly work and a popular one. The result
has been that
academic reviewers tend to find it accessible and engaging,
while reviewers
in more popular venues often agree with Rob that my book makes
considerable
demands upon the reader.

So, is Slade wrong in all his judgments? Nope, he is entitled
to his
opinions--and I agree that a couple of them are on target. But
since
numerous other readers and reviewers have reached rather
different
conclusions overall, I hope those curious will read my book and
judge for
themselves. My own view is that while my book is certainly
imperfect, it
addresses vitally important questions, and it remains the most
comprehensive
and incisive work written on its topic to date. (I guess I'm
not entirely
alone in that opinion; Rob's review neglected to inform RISKS
subscribers
that Democracy and Technology received the 1996 Don K. Price
Award of the
American Political Science Association as the "year's best book
on science,

technology and politics.") Thus, my suspicion is that whether one agrees with it or not, it's hard to read Democracy and Technology and not find oneself challenged to think about the social and political significance of technologies in a new, more illuminating way.

Thanks again to Rob Slade and to this forum.

Richard Sclove, Founder & Research Director, The Loka Institute,
P.O. Box 355,
Amherst, MA 01004 USA +1-413-559-5860 <http://www.loka.org>
Loka@amherst.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 20: Issue 12

Weds 9 December 1998

Contents

- [San Francisco power outage and Y2K](#)
[Cathy Horiuchi](#)
- [Air-traffic control comments](#)
[Paul Cox](#)
- [TCAS stories - 1 good, 1 bad](#)
[David Wittenberg](#)
- [Security risks of laptops in airline cockpits](#)
[Jim Wolper](#)
- [NW Frequent Flyer Miles subject to fraud](#)
[Sandy Antunes in PRIVACY Forum](#)
- [Another monster water bill](#)
[Brian Clapper](#)
- [Trusting non-redundant info about your RAID system](#)
[G.J. Dekker](#)
- [Export exemptions](#)
[Padgett Peterson](#)
- [Re: MS Outlook's calendar shifts with time zone](#)
[Stuart Lamble](#)
[Clive D.W. Feather](#)
- [Re: Spamming to Spy](#)

[Kevin Connolly](#)

● [Re: A risk ... of JavaScript](#)

[Steven M. Bellovin](#)

[Mathew](#)

● [Interesting effect of PG&E power outage](#)

[Greg Marriott](#)

● [Info on RISKS \(comp.risks\)](#)

✂ **San Francisco power outage and Y2K ([RISKS-20.11](#))**

horiuchi <horiuchi@ix.netcom.com>

Wed, 09 Dec 1998 11:15:59 -0800

The 8 Dec 1998 SF outage ([RISKS-20.11](#)) may be subject to as much scrutiny as the 10 Aug 1996 western states blackout ([RISKS-18.32](#)). Electric system deregulation has caused numerous changes in priorities. This outage is attributed to human error, a construction crew not knowing a pipe was acting as a ground. It could be considered an information error, if no sign, tag or other label were present and this sort of pipe is not routinely used (e.g., noted in standards and training manuals) as substation ground. www.euy2k.com today quotes PGN on this outage as a sample of the type of scenario problems which might result from Y2K remediation failures.

Is it a Y2K problem if utility executives decide it is preferable to spend \$50-100 million on a new customer billing system rather than spend that amount on tree-trimming, line-crew training, supervision, buyout of excess staff, or labeling of equipment in substations? Study of major

outages

suggests among key issues faced in electric system reliability are aging infrastructure and loss of the knowledge base on details of transmission and distribution systems when staff retires or is downsized out as part of deregulation. Starting a project to catalog and label every wire in every city has no glitz and few major consulting firm requirements. Yet this simple course of action will prevent many problems with the energy infrastructure, and could be included in the national infrastructure protection project (<http://www.ciao.gov>). The writings on complexity and system accidents of Charles Perrow are highly recommended.

Cathy Horiuchi, University of Southern California, formerly at the Sacramento Municipal Utility District, "Your Electric Service"

✈ Air-traffic control comments

"Paul Cox" <pcox@eskimo.com>

Wed, 9 Dec 1998 00:48:39 -0800

Hi. I'm an air-traffic controller at Seattle Center, located in Auburn, Washington. I am particularly drawn to RISKS reports of problems with the ATC system. I notice many times that, while generally accurate, there are some small but crucial errors in the general assumptions and conclusions drawn and made. For example, in [RISKS-20.11](#), there is a response to the Dulles radar failure issue. Steve Peterson says, in part:

> While radar failures are certainly important, it's wrong to say that radar failures deprive controllers of this information. In this situation, pilots report all three items (plus their position) to ATC via radio. ATC procedures provide for increased separation between aircraft to compensate for the lack of radar data.

> In the US (and presumably elsewhere), there are many places where reports by the pilot are the only source of information on the location of aircraft."

While fairly reassuring, this isn't exactly true. First of all, "radar" technically refers to the physical radar antenna; what we think of as ATC "radar" display scopes are typically mosaics of multiple radar sites. The physical radars themselves don't fail frequently at all; in fact, I've been working as a controller for almost 8 years now and have never had it happen.

What I HAVE had happen, numerous times, is failures of the various radar mosaic display systems, failures of the various communications systems, and power failures to the entire facility (which, of course, take absolutely everything. Except the cell phones in controller's cars.)

Getting back to what Steve Peterson said above, display system failures most certainly DO deprive controllers of data such as heading, speed, and altitude of aircraft. These three things are the most important, most crucial components to data controllers need to do their jobs.

In essentially all ATC facilities, printed or hand-written strips are required to be kept on each and every aircraft with needed data. In practice, however, controllers (particularly in busy terminal facilities) cannot keep those strips up to date. In practice, when working a busy "final" or "arrival" sector in a terminal facility, controllers are keeping the info on each plane in their head (which brings up some interesting single-point-of-failure questions.)

Controllers are indeed perfectly capable of controlling traffic through radio position reports, pencils, and their flight strips, as Mr Peterson suggests; however, the bad news is that it is much, much slower and inefficient. When the radar display unit fails, the controller scrambles to his strips, tries to recall which of them were actively being worked by him at the time, and re-establishes the "picture" in his head.

Good technique includes up-to-date strip marking; however, again, this is an area where practice often falls behind idealism. Staffing shortages might mean where, ideally, a controller working the radar will have an assistant handling all the strip-marking and landline calls (to other controllers to coordinate data); a controller might be normally capable of working a position alone, but be "down the tubes" temporarily and have fallen behind on his strip-marking; or he could simply be having a bad day.

What all this comes down to is that most of the time, there's not much

problem if the radar and/or radar displays fail. However, when they do (not if; history shows us they fail again and again and again, and shows no sign of abating) there is most definitely a temporarily greatly reduced safety factor.

The transition times immediately following a failure can be complete and utter chaos, and quite frankly would be quite terrifying to most pilots if they could see what's happening on the other end of that radio link.

Paul Cox, Enumclaw, Washington

✈ TCAS stories - 1 good, 1 bad

David Wittenberg <dkw@cs.brandeis.edu>

Wed, 9 Dec 1998 10:20:18 -0500 (EST)

In **The Boston Globe** on 8 Dec. and **The New York Times** on 9 Dec. (see [RISKS-20.11](#)) there is a story about two planes getting within 1.1 miles horizontally and 900 ft. vertically when they were supposed to be separated by at least 2 miles horizontally or 2000 ft. vertically. The planes were warned by their TCAS systems and avoided each other. The controller's union says they got too close in the first place because of a series of computer failures, the FAA says the incident is under investigation. Both planes were bound from the US to Europe and were talking to the Boston center.

[The **Globe** noted that there were 3 planes, and that when 2 of

the planes
changed course to avoid collision, one was then heading into the
third
plane.]

About a week earlier, there was a case where the TCAS told a Air
Ontario Dash 8 to climb to avoid a US air 737. The Dash 8 came
within
300 ft. of a Northwest A-320 whose TCAS told it to descend. In
this
case a controller noticed the "erratic" flight paths and
intervened.
Neither the Times nor the Globe explained why the A-320 was told
to
descend.

So the controllers got one pair of planes into a bad situation,
and
TCAS bailed them out; and TCAS got another set of planes into a
bad
situation and the controllers bailed them out. How are the
pilots to
know which one to trust when they must make decisions quickly?

David Wittenberg <dkw@cs.brandeis.edu>

✈ Security risks of laptops in airline cockpits

Jim Wolper <wolpjame@cwis.isu.edu>

Tue, 08 Dec 1998 06:49:02 +0000

The problem of laptop computer interference with flight and
navigation
equipment has been discussed in several issues of RISKS, notably
R-16.23 to
25, -18.46, and -18.52. Here is a new twist on that theme:
pilots wanting
to use laptops to interface with installed avionics. There are
several new
RISKS involved here.

INTRODUCTION

Pilots of transport-category and certain larger corporate aircraft use a system called ACARS to exchange text messages with designated receivers on the ground, usually a company dispatch office. ACARS can also be used to report maintenance anomalies, routine data on performance, and the like. The interface is awkward: I've observed experienced pilots swirl an index finger over the keyboard looking for a letter. And, ACARS messages are generally sent in clear text, that is, there is no encryption or other encoding. (ACARS is short for ARINC Aircraft Communications Addressing and Reporting System; ARINC is a company providing voice and data services to the air transport industry.)

Aviation Week and Space Technology now reports that Lufthansa German Airlines is now investigating the possibility of using "pilot laptop computers" and a dataport to ease the composition of ACARS messages. Such a course of action must be taken with extreme care: it opens a door to most of the known computer security problems.

Pfleeger's "Security in Computing" lists four security threats: interception, interruption, modification, and fabrication. The laptop-ACARS connection is vulnerable to all four, unless certain precautions are taken. These will be discussed at the end of the essay.

INTERCEPTION

As mentioned above, ACARS messages are transmitted in clear

text, and are subject to interception; in fact, there is a group of hobbyists who disseminate information about ACARS interception through a web site. Some argue that there is no value to intercepting ACARS messages (publicly owned airlines publish the economic data such as load factor, routes are standard, etc). Granting that this may be true for the airline, there are other parties which may be hurt by this information, primarily passengers.

Here is a true story. I was riding in the jumpseat of a major airline's Airbus A320 (one of my prerogatives as a professional pilot). A flight attendant came into the cockpit to report that a passenger had had a problem with his colostomy bag and wanted to stay in his seat after landing and have his luggage brought to him so he could change his clothes. The cockpit crew, quite sympathetic, sent an ACARS message to the dispatch office, which necessarily included the passenger's name. But ACARS messages are easy to intercept; I wonder if the passenger really wanted his name and the nature of his medical problem broadcast in the clear?

Ordinarily, there are no physical security problems with these messages but this is not the case with a pilot's laptop because presumably the composition of the message will be done on the laptop and the message will remain in the laptop. If the pilot then takes the computer home and allows his family to play with it, the size of the set of potential interceptors grows substantially.

INTERRUPTION

Once the laptop-ACARS connection is established as industry practice, any denial-of-service attack on the pilot's laptop becomes a denial-of-service attack on the airline. Such attacks include viruses and worms. Similarly, power supply, disk controller, or battery problems have the potential to disable the system at the laptop interface.

MODIFICATION

One modification issue involves the physical security of the laptop. Again, a virus or worm could be introduced which would alter the program encoding ACARS messages. Other modifications include changes to company manuals stored on the laptop.

Modification becomes a more crucial issue when the laptop is actually connected to the airplane's avionics; one needs to be sure that this connection can't modify other aspects of the on-board avionics.

FABRICATION

The ACARS data link, since it is cleartext, is subject to bogus messages transmitted in either direction. Some airlines use ACARS to transmit weight-and-balance data to the aircraft, and the aircraft's trim is set before takeoff based on this information. If the crew receives false weight-and-balance data, the trim might be set incorrectly. This has caused many accidents, most recently the Fine Air DC-8 freighter which crashed leaving Miami.

AVOIDING PROBLEMS

Pilots are frustrated with the ACARS interface and are correctly looking for ways to improve it. The laptop connection could be secure if the following precautions are taken:

1. Ensure physical security of the laptop. It is not the pilot's laptop, it is the company's laptop, and does not go home with the pilot. It stays on the airplane or in the dispatch office. This reduces the RISK of all four threats.

2. Ensure communications security by using a simple cryptography scheme. The RISKS are short-lived, so even a simple crypto scheme that can be broken in a few hours is a major improvement. It should be noted that Scandinavian Air Systems is already implementing crypto in its ACARS messages, by adding hardware and software to the unit on the airplane. For verification purposes, a checksum such as MD5 or a public-key digital signature would provide more than adequate security.

CONCLUSIONS

The SAS example makes something more clear, namely, that there are two problems with the system: the interface and the plaintext transmission of the data. SAS's crypto addresses the latter but not the former. The laptops address the former but not the latter.

The ACARS interface problem is a real one, but trying to solve it by adding

yet another level of technology does not seem to be the best way to solve.

Jim Wolper ATP/PhD/CFI, Department of Mathematics, Idaho State University
Pocatello, ID 83209-8085 +1 208 236 2453 <<http://math.isu.edu:80/~wolperj>>

[Jim Wolper requested that a note be added to the archive copy:
The source for this information on SAS was a copyrighted story
in "Air Transport Intelligence", an on-line journal.
PGN]

✈ NW Frequent Flyer Miles subject to fraud

Sandy Antunes in PRIVACY Forum <privacy@vortex.com>
Sat, 5 Dec 98 12:58 PST

From the PRIVACY Forum Digest V07 #19 5 Dec 1998

Date: Tue, 27 Oct 1998 16:32:59 -0500
From: antunes@xeno.gsfc.nasa.gov (Sandy Antunes)
Subject: NW Frequent Flyer Miles are publically accessible-- and usable

Flyers beware-- I've run into a severe privacy/security hole in Northwest's frequently flyer program, "WorldPerks"-- one that NW is not interested in changing.

The short summary is, it seems anyone who knows your phone number can use your Northwest "WorldPerks" frequent flier miles to get an E-ticket issued in their name with your miles (or can simply find out your mileage balance). This is intentional, by design.

I found this out when my mother was able to upgrade a "gift"

ticket I

gave her to First Class-- using my miles-- without my authorization.

It turns out that it doesn't even have to be a relative or someone you got a ticket for-- just someone who knows your phone number.

The record of this transaction (a receipt) is provided as the only notification of the transactions. Tickets issued can be for travel as soon as 4 days in the future (at which point the receipt is FedExed or faxed) or over 14 days in the future (receipt is just sent postal mail). In my case, 3 weeks passed between the ticket request and arrival of a receipt.

The privacy concerns are this:

- anyone can get your frequent flyer mileage balance knowing only your phone number,
- anyone can deplete your mileage balance with malicious intent, knowing only your phone number, and
- the only sign that a ticket was issued is a receipt mailed by post, so people with open mailboxes, people changing addresses, people on vacation, bosses with secretaries, and people with housemates are easy prey to having their miles stolen without knowing.

Unlike credit card fraud, NW does not consider banked miles as currency, and it is the account holder's responsibility to find and file fraud charges against the ticketholder. 1st line managers have the option of waiving the \$35 'rebank' fee if you wish to cancel such a ticket, if the flight has not already occurred.

The most likely safeguard-- that only the person who owns the frequent flyer account can request a ticket be issued-- is not something NW will consider. Quoth Jay (with permission), "The system is a great system, and it works, and we don't have problems with it. You're taking a situation that happened to you, and trying to completely blame it on Northwest, and I don't appreciate it."

So, your account information is available to anyone who has access to a phone book (a privacy concern), the actual balance can be tampered with by same (an authorization risk), and catching such deeds is the responsibility of the account holder (verification after the fact).

"Some People Just Know How to Fly", indeed.

Sandy Antunes <antunes@xeno.gsfc.nasa.gov>

[For subscription information for the PRIVACY Forum Digest, see [RISKS-20.00](http://catless.ncl.ac.uk/Risks/20.00.html) <URL:<http://catless.ncl.ac.uk/Risks/20.00.html>>. PGN]

⚡ Another monster water bill

Brian Clapper <bmc@WillsCreek.COM>
Tue, 8 Dec 1998 13:51:12 -0500 (EST)

Courtesy of a friend of mine who lives near Seattle:

> Earlier, I wrote:
>
>> We just received our monthly water bill...

>> and it was for \$18121.85 !!! The water company says it's
>> switching to a new computer system and to ignore the bill.
>
> Well, we just received a Past Due notice, threatening to turn
off our
> water if we don't pay the above amount plus a 10% late-payment
penalty
> of \$1812.19; this brings the total to \$19934.04! As before,
when we
> phoned the water company, they said to ignore the bill ...
we'll see
> what happens!

History just continues to repeat itself.

Brian Clapper, bmc@WillsCreek.COM, <http://WWW.WillsCreek.COM/>

⚡ Trusting non-redundant info about your RAID system

"G.J. Dekker" <gjdekker@nlr.nl>
Wed, 09 Dec 1998 09:03:10 +0100

A few weeks ago one of the 8 disks in a RAID-5 cabinet on our PC server failed. The only indication of the identity of the defunct disk was in the graphical interface software on the operators console, which was a perfect look-alike of the physical cabinet. The console indicated that the third disk of the upper row of four was faulty. However, after replacing this disk, the system crashed. After reboot, it appeared that now the third disk of the upper row still was defunct, and that in addition the third disk of the lower row did not contain information.

It took quite some amount of effort and luck to find that the

graphical
interface software had interchanged the two rows, such that in
effect one of
the functional disks was replaced, while there was no redundancy
left due to
the other failed disk. The whole process of finding the cause of
the problem
an solving it led to an outage of the server of about 6 hours.

The risk: even in a properly designed redundant system there can
be
non-redundant pieces. Trusting non-redundant info on your system
can be
dangerous.

G.J. Dekker -- National Aerospace Laboratory (NLR), Informatics
Division
P.O.Box 153,8300 AD Emmeloord, The Netherlands +31 527 248435
(operator 248444)

Export exemptions

"Peterson, Padgett" <padgett@gdi.net>
Wed, 09 Dec 1998 08:37:23 -0500

>The Norwegian developer Eivind Eklund wrote on slashdot.org:
> I just got information on how Norway (where I live) implement
this
> (ie, how the regulations are changed). The new rules prohibit
export
> of crypto-software, but with a deliberate exception for open
source
> software.

This is quite interesting since the implementation of the crypto
algorithms
is really the boring part of programs like PGP. While people
once did not
mind comand line interfaces and "pgp -sea <file>" was
meaningful, today the

crypto is a minuscule piece of programmes. In 1994 when the "Enclyptor" was introduced, I told Dave that this was the future. Today we have key servers, tray icons, and Eudora/Exchange plugins, none of which contain "crypto" yet are what will make or break a product commercially.

Sounds like all that is necessary to make public is an API that contain the various crypto modules while the wrappers that provide the GUIs and automatic execution (the moneymakers) remain proprietary.

Padgett

✉ Re: MS Outlook's calendar shifts with time zone (Marriott, R-20.11)

<slamble@csc.com>

Wed, 9 Dec 1998 14:05:22 +1000

Been there, done that, got the T-shirt. It happens with just about everything you care to name under Outlook's calendar, including recurring appointments -- that's where I first noticed it. I'd enter an appointment for (say) 8:30pm to 9:30pm on a Tuesday, recurring every week until the end of time. Surprise -- daylight saving finishes, and all of a sudden, the appointments are for 7:30pm to 8:30pm. Even "events" (full-day happenings -- e.g., birthdays) aren't immune, so I was mildly amused to notice that a number of events started at 1am some days, midnight others...

Maybe they were just taking a leaf out of Lotus' book? Lotus

Notes does

something similar; it has been demonstrated for e-mail (date sent is displayed relative to your timezone rather than the timezone it was sent), and it wouldn't surprise me if the calendar aspect of it does something similar.

It's one of those things that, in my opinion, should be configurable. I'm

not familiar with American time zones, so I'll give an Australian example:

Perth is three hours behind Melbourne, two and a half hours behind

Adelaide. Suppose somebody in Perth wants to set up a telephone meeting with

somebody in Melbourne and somebody in Adelaide. They might say "10 am". Do

they mean 10 am Perth time, Adelaide time, or Melbourne time?

With a feature

like this, the Perth guy can say "10 am", and it gets translated to "1 pm"

for the Melbourne guy behind the scenes (12:30pm for the Adelaide chap.) I'm

not saying it's always a Good Thing(tm) -- just that sometimes it's

appropriate, sometimes it isn't.

Of course, this is just another recurrence of the perennial question: how

far should software go in trying to second-guess the person operating the keyboard?

Stuart Lamble

⚡ Re: MS Outlook's calendar shifts with time zone

"Clive D.W. Feather" <clive@demon.net>

Wed, 9 Dec 1998 11:31:17 +0000

I've used systems that do the opposite - store all appointments in the local time for the system. You get to meetings in New York on time, but the alarm for the urgent phone call to someone in London is 5 hours late because it went off at 1500 EST instead of 1500 GMT.

There's no easy way to win here, other than having an explicit "not this time zone" flag on diary systems.

Clive D.W. Feather, Director of Software Development, Demon Internet Ltd.

Tel: +44 181 371 1138 Web: <<http://www.davros.org>>

[Other comments on this subject from eight others! The bottom line is specify your frame of reference. PGN]

✶ Re: Spamming to Spy (Mills, [RISKS-20.11](#))

Kevin Connolly <Kevin.Connolly@ansf.alcatel.fr>

Wed, 09 Dec 1998 11:38:59 +0000

In [RISKS-20.11](#) Dick Mills wrote of the possibility of audio/video Trojans.

It has already been done. "Back Orifice" from the "Cult Of The Dead

Cow" <http://www.cultdeadcow.com/> is a trojan that includes the feature to find your PC attached camera and take a picture (still or video).

<http://www.cultdeadcow.com/tools/bo.html>

Kevin Connolly, EI4ANB

⚡ Re: A risk ... of JavaScript (Thompson, [RISKS-20.11](#))

"Steven M. Bellovin" <smb-lists@research.att.com>

Wed, 09 Dec 1998 08:44:23 -0500

There are many sins that can be ascribed to JavaScript, but this flaw is ubiquitous on the Web. There are very many ways for Web sites to send you to other places, ranging from JavaScript to embedded images (including those from "adult" sites) to http-level redirects. The real question, one that is asked by the browsers to the Web sites, is "where do I want to go today?"

⚡ Re: A risk ... of JavaScript (Thompson, [RISKS-20.11](#))

mathew <meta@pobox.com>

Wed, 9 Dec 1998 14:53:49 -0500

Of course, a survey which only samples opinions from readers who happen to have JavaScript enabled is so obviously statistically flawed that it's a bit pointless doing it in the first place.

⚡ Interesting effect of PG&E power outage ([RISKS-20.11](#))

Greg Marriott <greg@spies.com>

Tue, 8 Dec 1998 13:18:39 -0800

San Francisco and San Mateo counties in California suffered a massive power loss on the morning of 12/8/98.

I live in nearby Palo Alto, a community not directly affected by the outage.

My Mitsubishi television equipped with TV Guide+, however, forgot all of its stored programming information. TV Guide+ is an online television program guide. The television schedule is updated automatically several times a day by tuning to a local public broadcasting station and downloading the next few days worth of programming.

In my case the PBS station is KQED channel 9 in San Francisco. I assume they lost power along with the rest of the peninsula and the Guide+ service was disrupted.

Apparently when my television failed to connect to the information server it decided the best reaction was to dump everything. I find this failure mode a bit annoying because the television stores enough data for 2 or 3 days worth of viewing. I would have preferred that it wait for a few more update cycles before deciding the server was gone for good. Now I not only have to re-enable TV Guide+, but I have to wait for about a day for the full schedule to be downloaded. And then I have to go through all the available channels, again, and disable the ones I don't need. (this leaves more memory for program descriptions on the channels I *do* need)

Greg Marriott



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 13

Thursday 24 December 1998

Contents

- [Near-miss at LaGuardia Airport, NYC](#)
[Dave Weingart](#)
- [Runaway train on Capitol Hill](#)
[Thomas A. Russ](#)
- [Another fibre-optic cable cut](#)
[Bob Blanchard](#)
- [British Government admits Y2K missile problem](#)
[Phil Pennock](#)
- [2,000 Texans get false overdraft notes in Y2K test](#)
[Bill Bauriedel](#)
- [Wassenaar Agreement exempts 'public domain' software](#)
[Martin Hamilton](#)
- [Other infrared security crocks](#)
[Paul Wexelblat](#)
- [Re: PalmPilots voiding car locks in Europe](#)
[Philip Koopman](#)
- [E-LIFE'S RISKS? I.R.S. E-FILE!](#)
[Andrew Greene](#)
- [Should pilots trust TCAS?](#)
[Andres Zellweger](#)

- [Airlines databases lock in increases better then refunds](#)
[Peter](#)
 - [Re: Frequent Flyer miles accessible](#)
[Peter](#)
 - [Y2K expansion](#)
[Jerry Leichter](#)
 - [Intelligent virus invades NT servers](#)
[Edupage Editors](#)
 - [Unexpected date behavior in Windows 95](#)
[Daniel Weber](#)
 - [Microsoft Trojan Horse](#)
[Frank Markus](#)
 - [Quark XPress, hates Unix scripts!](#)
[Ben Sherman](#)
 - [Password hint risks](#)
[Alexander V. Konstantinou](#)
 - [Risks in incorrect warnings and alerts](#)
[Flint Pellett](#)
 - [CFP: 1999 National Information Systems Security Conference](#)
[Ed Borodkin](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈ **Near-miss at LaGuardia Airport, NYC**

Dave Weingart <dweingart@chi.com>

Thu, 10 Dec 1998 09:24:40 -0500

According to reports I heard on the radio this morning, a US Airways Boeing 737 came less than 100 feet (some reports say within 50 feet) landing on smack on top of a small corporate plane at LaGuardia Airport in New York City on Wednesday, 2 Dec 1998. The passenger flight was given permission to land, despite the fact that the smaller plane was waiting to take off on the

same runway. The near-disaster has been blamed on too few controllers being too distracted.

Dave Weingart, Strategix Solutions dweingart@chi.com 1-516-682-1470

✈ Runaway train on Capitol Hill

Thomas A. Russ <tar@ISI.EDU>
17 Dec 1998 13:52:45 -0800

I found the following item in the *Los Angeles Times* 16 Dec 1998.

Especially intriguing are the spokesman's comments. There is also the nagging question of why there is an operator on a fully automated system in the first place.

...there IS a runaway train on Capitol Hill. The automatic brakes on the Senate subway between the Russell Office Building and the Capitol failed last week, sending the train crashing into a wall and slightly injuring the operator and the two other people on board. In the best congressional spirit, a spokesman for the architect of the Capitol stressed that "there was no operator fault involved. It's all automatic," said Herb Franklin, "and it's supposed to stop by itself."

Thomas A. Russ, USC/Information Sciences Institute
tar@isi.edu

⚡ Another fibre-optic cable cut

Bob Blanchard <b.blanchard@computer.org>

Wed, 09 Dec 1998 22:07:20 -0500

My office's frame relay link to our corporate WAN was out for a day on 26

Nov 1998. As it turns out, we were not alone. A railway backhoe operator accidentally cut an AT&T Canada fibre cable along the rail line between

Toronto and Windsor, crashing computers, knocking out phone lines, and

generally disrupting communications in southern Ontario. The main branch of

the Bank of Nova Scotia was computerless. Rerouting of Internet lines via

the U.S. was slow because of the Thanksgiving holiday. [Source: Veronique

Mandal, ``Cut Cable Paralyzes Network - Severed line brings hi-tech to its

knees'', *Windsor Star, London Free Press, Chatham Daily News*, 27 Nov 1998;

PGN Abstracting]

⚡ British Government admits Y2K missile problem

Phil Pennock <phil@athenaeum.demon.co.uk>

Wed, 9 Dec 1998 23:03:55 +0000

From The Times, 9 Dec 1998, p2:

Bug threat to missile

The Ministry of Defense admitted for the first time that the millennium bug

could have left Britain vulnerable to air attack. It discovered that the

Rapier anti-aircraft missile would have failed to retaliate.

The problem was identified inside the field equipment which activates the missiles and it would have made the system inoperable. The threat to Britain's defenses posed by the computer bug was outlined by George Robertson, the Defense Secretary. [Well, at least the failure mode was to not fire.]

🔥 2,000 Texans get false overdraft notes in Y2K test

"Bill Bauriedel" <Bill.Bauriedel@Forsythe.Stanford.EDU>

Fri, 18 Dec 98 10:47:21 PST

2,000 Texans get false overdraft notes in Y2K test
Reuters, Detroit News, 12/17/1998

Bank One Texas was testing their Y2K systems to see if they could send out overdraft notices after "1/1/00". They were able to print over 2,000 fabricated notices. But someone forgot to throw away the printouts, which were mailed out! <<http://www.detnews.com/1998/technology/9812/17/12170189.htm>>

🔥 Wassenaar Agreement exempts 'public domain' software

Martin Hamilton <martin@net.lut.ac.uk>

Fri, 11 Dec 1998 17:00:48 +0000

Just to note that the Wassenaar Agreement explicitly exempts 'public domain' software, in its 'General Technology Note':

Controls do not apply to "technology" "in the public domain",

to
"basic scientific research" or to the minimum necessary
information
for patent applications.

The 'General Software Note' has this to add:

The Lists do not control "software" which is either:

1. Generally available to the public by being:

a. Sold from stock at retail selling points without
restriction,

by means of:

1. Over-the-counter transactions;
2. Mail order transactions; or
3. Telephone call transactions; and

b. Designed for installation by the user without further
substantial support by the supplier; or

N.B. Entry 1 of the General Software Note does not release
"software" controlled by Category 5 Part 2.

2. "In the public domain".

See <URL:<http://www.wassenaar.org/List/GTNGSN.doc>>. Category 5
is the
section on 'Information Security', of course. Last updated 10th
December 1998.

"In the public domain" is defined as:

This means "technology" or "software" which has been made
available

without restrictions upon its further dissemination.

N.B. Copyright restrictions do not remove "technology" or
"software"

from being "in the public domain".

See <URL:<http://www.wassenaar.org/List/Def.doc>>.

Martin

✶ Other infrared security crocks

Paul Wexelblat <wex@cs.uml.edu>

Thu, 10 Dec 1998 11:52:02 -0500

The discussion in [RISKS-20.10](#) about theft of infrared codes for door locks brings to mind two similar issues.

1. Conventional RF garage door openers left in cars at parking/repair garages are easily opened so "the baddies" can see the code and program a "universal" opener to get in -- many folks don't lock the door between their garage and house.
2. My household internal alarm system uses coded infrared beams. These are trivially defeated with one of those X-10 type "control extenders". A device (you may have seen them, they're 3" pyramid shaped things) that you zap your IR remote control at, this device converts the signal to RF that goes through walls and the receiver reconverts and emits IR to the sensor. (I use one to control my cable box from the bedroom.)

Using this thing I can just put the pair between the alarm transmitter and receiver and walk on through.

...wex

⚡ Re: PalmPilots voiding car locks in Europe (McCoy, [RISKS-20.10](#))

Philip Koopman <koopman@cmu.edu>

Thu, 10 Dec 1998 03:43:17 GMT

I have heard that one can get stand-alone "diagnostic" boxes to record and play back transmissions for the RF car interfaces. In fact, in response to this some vehicles with RF interfaces already have cryptographic encoding of transmissions (I designed such a system with Alan Finn back in my industrial research lab days, and it is in moderately wide use in some US vehicles today).

One of the RISKS of this area is that in general the market won't currently bear the cost of high-strength cryptography -- they only get a few cents extra to spend on it, and even something like DES tends to cost too much. So it is difficult for consumers to evaluate whether they're getting crypto that is strong enough to be reasonable for the application, or one of the systems that says it is but really isn't (or one of the systems that really is but competitors claim it isn't, or ...).

Phil Koopman -- koopman@cmu.edu -- <http://www.ece.cmu.edu/~koopman>

⚡ E-LIFE'S RISKS? I.R.S. E-FILE!

Andrew Greene <agreene@bitstream.com>

Thu, 10 Dec 1998 11:16:38 -0500

I received a postcard this weekend from the Internal Revenue Service, notifying me that my wife and I have been selected to (optionally) participate in a pilot implementation of the new, improved "e-File". This is a way of electronically filing our income tax returns next April, where not only is the information transmitted electronically and the payment or refund handled via EFT, but we will not even be required to mail in a signature card.

Instead of the physical signature card, we can simply use the electronic "signature" number enclosed in a sealed section of the postcard that we received this weekend. (The number is only five digits, but for a one-time use that's probably not too bad.... right?)

It's an old story, I know, but one which apparently bears repeating, because organizations are still doing it. This piece of mail was unsolicited, so had someone pilfered it from my mailbox and used it to file a false return, *I* would have been the one in trouble with the IRS.

- Andrew Greene

[Nice palindromic subject line (ignoring punctuation)! PGN]

✶ Should pilots trust TCAS?

Andres Zellweger <ZellwegA@cts.db.erau.edu>

Thu, 24 Dec 1998 10:14:08 -0500

In [RISKS-20.12](#) David Wittenberg reported on two situations, one where TCAS may have created an incident that was "saved" by air traffic controllers and another where air traffic controllers may have created an incident that was "saved" by TCAS. He asks "How are pilots to know which one to trust when they must make decisions quickly?"

I recently completed a case study on TCAS for a graduate seminar on building safe systems. My students and I were convince, after looking at the extensive TCAS safety activities over the last 15 years, that TCAS is indeed a very effective "safety net" for pilots.

After TCAS introduction began, it became clear that a clear set of TCAS operational procedures for both pilots and controllers was necessary to get the full safety benefits of TCAS. For instance:

- "pilots should follow resolution advisories unless doing so jeopardizes the safe operation of the flight or the flight crew has definitive visual acquisition of the intruder."

- "when responding to a resolution advisory hat directs a deviation from an ATC clearance, pilots should communicate with ATC as soon as possible."

- "after a controller has been informed that an aircraft is responding to a resolution advisory, the controller should not issue control instructions to that aircraft that are contrary to the resolution advisory."

and so on ...

I would personally be very upset if pilots, at this stage in the evolution of TCAS did not follow TCAS resolution advisories. The probability of TCAS errors is very small compared to the likelihood that an air traffic control countermand to a TCAS advisory will lead to potential problems.

Unfortunately, I have not seen any reports of the FAA's (or anyone else's) investigation into the former (more interesting, from a safety perspective) incident. The good news is that analysis of reported incidents like this has historically continued to lead to TCAS improvements. The bad news is that the FAA's investment banker has not seen it fit to continue funding of the ~TCAS Program at levels sufficient to continue TCAS improvements. Indeed, there are some who have questioned whether the safety analysis of the new TCAS version 7.0 (developed primarily for use in European airspace) has been adequate.

✈ Airlines databases lock in increases better than refunds

<peter@hightown.demon.co.uk>

Sat, 12 Dec 1998 22:43:47 +0000

Earlier this year I had occasion to return from Johannesburg to London on business. I was booked business class for this journey. On the flight day the airline was a plane down so I and a colleague were transferred to

economy on the next plane. All the paperwork was completed and entered into computer on check-in.

When I returned to the office I asked the staff who deal with travel to verify with our travel agent that the downgrade was credited with a refund to the business. This did not happen. Full fare was charged. It took many months to unsnarl the paper trail and it was not clear who should have informed who about what. The way the legalese on tickets is written maybe it was all our fault for traveling!

It took us many man-hours to resolve the situation and probably many business travelers do not bother assuming that "the system" sorts out little details. But when "the system" comprises the IS systems of several travel firms and subcontractors programmed to bill any upgrades or additions exactly it only takes one to fail to pass on refunds to give a "heads you lose" situation. Just like the vending machines -- they never dispense free drinks but there are often stickers on them saying, "it owes me 17p" (UK pence).

⚡ Re: Frequent Flyer miles accessible ([RISKS-20.12](#))

<peter@hightown.demon.co.uk>
Sat, 12 Dec 1998 22:43:47 +0000

I find the quote from NW surprising in view of the fact that the BA

"Airmiles" accounts can only be used from the WWW with an initial PIN sent by snail mail to the account holder's address. Changing the PIN can only be done online using https: access.

Unlike in the US, in Britain there is popular reluctance to adopt universal ID such as by Social Security number or phone number.

⚡ Y2K expansion

Jerry Leichter <leichter@lrw.com>

Sun, 13 Dec 98 08:21:25 EST

As not-particularly-competent (but professionally paranoid) lawyers have gotten more and more heavily involved, the range of "Y2K critical" dates has grown. A story has made the rounds that some software uses "9999" in the date field to indicate special processing; hence, software is now supposed to be tested for proper operation on 9 Sep 99. (Why operation *on that date* should be affected is beyond me. Then again, since a date written with a two-digit year and no separators necessarily has to be stored in at least a 7-digit field -- there being at least one month with a month number larger than 9 containing at least one day with a number larger than 9 -- it's beyond me why one would expect software to use 9999 as a flag; 9999999 is much more likely, and completely safe.)

I recently saw proposed language that would require a vendor to certify proper operation on about 15 dates, starting with 9 Apr 1999 and

ending some
time in 2002. One could make a rough kind of sense of many of
the dates --
e.g., they tested proper leap year handling in 2000 and
thereafter -- but
some of them are real head-scratchers. The 9 Apr 1999 date is
one of those.
Is it that 4 and 9 look alike, so that 9499 (or is it 4999?)
might have been
used as a magic flag? :-)

I worked with a lawyer doing Y2K requirements for a major
corporation, and
convinced them not to put *any* explicit date requirements in.
Rather, the
language is all written in terms of proper operation on any
dates, and with
any input date data, that will foreseeably arise in normal
system operation
during the expected lifetime of the system. Not only does this
avoid
getting into silly "my list of dates is longer than yours, hence
you weren't
exercising due diligence" games, but it also avoids a genuine
bug in the
way most of these provisions have been written: They focus so
closely on
dates around the year 2000 that they ignore the possibility of
problems with
dates further away. For example, a vendor could introduce
windowing -
continue to store two-digit years but have 50-99 always
represent 1950-1999
while 0-49 represent 2000-2049 - to easily comply with most Y2K
requirements
I've seen. That's fine if the field in question represents
order dates, but
not so good if it represents dates of birth.

-- Jerry

⚡ Intelligent virus invades NT servers

Edupage Editors <edupage@franklin.oit.unc.edu>

Tue, 22 Dec 1998 14:22:43 -0500

A new computer virus that attacked 10 MCI Worldcom networks last week is capable of spreading throughout computer networks and scrambling the documents on those networks as it goes. "We've never seen anything this sophisticated in 10 years of doing this," says Network Associates' general manager of network security. "This is a completely new strain of virus and the first we've seen that propagates itself with no user interaction." The "Remote Explorer" virus runs on Microsoft Windows NT servers and affects common programs like Microsoft Word. Users clicking on their Word icon might experience a slight delay, but otherwise would be unable to detect the presence of the virus; meanwhile, the virus is busy corrupting files and spreading to other programs. Microsoft officials say they're "aware of other viruses that have the same characteristics," and Network Associates says it has developed a Remote Explorer detector and is working on a solution to decode the affected files. (*Wall Street Journal*, 22 Dec 1998, Edupage, 22 December 1998)

[Sounds like a worm to me. PGN]

⚡ Unexpected date behavior in Windows 95

Daniel Weber <djweber@sandstorm.net>

Wed, 16 Dec 1998 18:21:46 -0500

I came across the following interesting behavior in Windows 95:
if you use
the "Date/Time Properties" dialog box to change the month or day
of month,
the system clock is actually set to that date, without the user
hitting "OK"
or "Apply."

The risk is that the user is changing system properties without
really being
aware of it--if the user hasn't pressed "Apply" he or she will
figure that
the change hasn't occurred yet. Although pressing "Cancel" will
restore the
date, any applications that check the system clock in the
meantime will read
the altered system time.

As a simple example, consider a mail reader that checks for new
mail every
five minutes by comparing system times. If it checks mail
during an
interval when the clock is set forward a day and then reset, the
mail reader
will not check mail again for 24 hours.

I don't know how many applications expect and rely on the system
time
to be monotonically increasing.

I've been told that other Windows dialogs, besides the date/
time, also
prematurely change system settings in similar ways, but I'm not
sure what
implications other settings may have.

I tested this on an NT machine and on a Windows 98 machine that
was said to
have the recent Y2K patch installed, and noticed the same
behavior.

Dan Weber, Sandstorm Enterprises, Inc. <http://www.sandstorm.net/>
1-617-547-0011 djweber@sandstorm.net

⚡ Microsoft Trojan Horse

"Frank Markus" <fmarkus@pipeline.com>

Thu, 10 Dec 1998 21:33:24 -0500

I am running Win98 with a Microsoft module that automatically notifies me of "critical updates" and takes me to a Microsoft Updates web site. The first item on the list of updates was one that was intended to make Win98 Y2K compliant. This module was roughly 1.5MB. Further down the list was a beta IE virtual machine (presumably designed to comply with the Sun Java decision.) This file was roughly 4MB; I decided to pass on it. Having specified what I wanted to download -- and install (it is both or nothing) -- I noticed that the download was going slowly. And then I discovered the reason: the file that I was downloading was over 5MB ... and included the Virtual Machine Beta that I had not checked! I cancelled the download and went back to check whether I had made an error. I had not. I repeated the exercise with the same result.

My conclusion is that in an effort to show 'good faith' compliance with the Sun Java court order, Microsoft is installing the revised Java engine on the computers of users who have decided against using it. The cheese that they

are using to bait their trap is the promise of Y2K compliance.

Does anyone who is using Win 98 and the IE 5.0 beta know how to get only the Y2K update?

✂ Quark XPress, hates Unix scripts!

Ben Sherman <ben@2600.com>

Wed, 9 Dec 1998 21:28:10 -0500 (EST)

Recently, we at 2600 Magazine published an article with a few Unix scripts in it.

A neat feature of XPress is that it allows you to put XPress specific formatting using plain ascii text, i.e. <i> for italics, for bold and so on. So what do you do if you need to you the > or < symbols (in a script for instance)? Easy, XPress just looks for 2 > or < in a row.

So when you print something that says:

```
echo "root2:x:0:1:Root:/:/sbin/sh" >> /etc/passwd
```

it gets truncated to

```
echo "root2:x:0:1:Root:/:/sbin/sh" > /etc/passwd
```

In unix, >> appends something to a file, and > replaces the file, so any command in a script to append something to the end of a file, would actually ERASE the file and REPLACE it with the one thing that was supposed to be added.

Eeek!

⚡ Password hint risks

"Alexander V. Konstantinou" <akonstan@cs.columbia.edu>

Fri, 11 Dec 1998 12:29:51 -0500

In the process of using the Netscape 4.5 automatic update feature I was asked to join the Netscape Netcenter. The form requests that you supply an account name, password, name, electronic as well as physical address (to be fair, you are given several options on how this information can be used).

The unusual aspect of this form, was an option to include a password hint with the following explanation :

"If you forget your password, Netcenter will present you this password hint to help jog your memory. Example hint:
'same password as my bank acct.' "

The risks are clear : potential access to your name, address and bank PIN !

Alexander V. Konstantinou

[Various comments received on this one. TNX. PGN]

⚡ Risks in incorrect warnings and alerts

Flint Pellett <flint@kai.com>

Wed, 16 Dec 1998 18:02:34 -0600

It seems to me that more often than not, the reason a Risk rears

its ugly
head is because either somebody wrote a piece of software
without thinking
about what possible states exist for various variables, or (a
pet peeve of
mine), somebody issued an incomplete error message, or both.
[My definition
of a "complete" error message is one that tells me not only what
is wrong,
in a way I can be expected to understand, but also gives me some
clue what
to do to fix it or where to go to get help.]

While the example below is a trivial Risk (I hope), it
illustrates
both of the above quite well.

I just installed my copy of the 1999 version of a widely used
personal
finances software package, and migrated data from a much older
version
without incident. The new version includes a new feature (new
to me anyway)
to show alerts if my charge card balances are "near my credit
limit." I was
very surprised, on my first entry, to see an alert telling me
that one of my
cards was near my credit limit. I was even more confused when I
examined
the account: my balance owed was \$0!

I eventually figured out their default algorithm for those
alerts, by
examining several other accounts. They would take the account's
credit
limit, subtract \$3,000, and set the resulting value as the
default upper
limit on the balance owed before an alert would be issued. That
made the
default on my gasoline company card with its \$700 credit limit
be negative
\$2,300. [Feel free to draw your own conclusions about the
person who came

up with `_that_` algorithm.]

When I found the place where you can change those defaults, the offending account wasn't listed, so I can't fix the -2,300 value. I suspect that perhaps someone used a negative number in that field to decide that this account isn't a credit card account and shouldn't be in the list. I appear to be stuck with this incorrect warning message until such time as the gas company owes me more than \$2,300 on the account.

As for that (scary) error message, "Account XXX is near your credit limit", it could have almost trivially been presented to me as the following: "You owe \$0 on Account XXX, which has a \$700 limit. You will see this alert whenever your balance exceeds \$-2,300." The first message wasted a considerable amount of my time in having to figure out what was going on. The second would have made it a lot easier, if not obvious, and would certainly have generated less stress. Millions of people use this program- millions of minutes can get wasted when people can't figure out what is triggering a warning. Is that a trivial Risk? Maybe not.

Can I conclude anything else about this incident? Yes. The QA people who tested this, who apparently don't have any charge accounts with credit limits under \$3,000, are quite likely overpaid. :-)

--Flint Pellett

CFP: 1999 National Information Systems Security Conference

"Ed Borodkin" <borodkin@constitution.ncsc.mil>

Fri, 18 Dec 1998 14:43:26 -0500

The National Information Systems Security Conference (NISSC) welcomes

papers, panels, and tutorials on all topics related to information systems security. Our audience represents a broad range of information security interests spanning government, industry, commercial, and academic communities. Papers and panel discussions typically cover:

- * research and development for secure products and systems, presenting the latest thinking and directions;
- * electronic commerce;
- * legal issues such as privacy, ethics, investigations, and enforcement;
- * practical solutions for government, business and industry information security concerns;
- * network security issues and solutions;
- * management activities to promote security in IT systems including security planning, risk management, and awareness and training;
- * implementation, accreditation, and operation of secure systems in a government, business, or industry environment;
- * international harmonization of security criteria and evaluation;
- * evaluation of products, systems and solutions against trust criteria;
- * tutorials on security basics and advanced issues;
- * security issues dealing with rapidly changing information technologies;
- * highlights from other security forums; and
- * implementing policy direction.

For more details see <http://csrc.nist.gov/nissc/call.htm>.

[The most important detail: the deadline
for submissions is 15 Feb 1999. 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 20: Issue 14

Sunday 3 January 1999

Contents

- [Car computer directs couple into river](#)
[PGN](#)
- [Swedish passport system struck by 99](#)
[Ulf Lindqvist](#)
- [Swedish Giroguide also hit by 99](#)
[Martin Minow](#)
- [Excel bug](#)
[Tom Rowe](#)
- [Chinese sentence hackers to death](#)
[John Knight](#)
- [Student can criticize school on web site, judge says](#)
[Declan McCullagh](#)
- [Hackers have fun with Furby](#)
[Robert Raisch via Dave Farber](#)
- [Now you see it, now you don't](#)
[Jerry Leichter](#)
- [Y1999: Risk of re-using data fields for error signaling](#)
[Daniel A. Graifer](#)
- [99-Year retrospective health insurance - or Y2K problem](#)
[Fraser McHarg](#)

- [San Francisco power outage and the risks of signs](#)
[Eric Leif](#)
 - [Page-layout program hazards](#)
[Jordin Kare](#)
 - [Some new things to try at all.net](#)
[Fred Cohen](#)
 - [Privacy Digests](#)
[RISKS moderator](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Car computer directs couple into river**

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

Mon, 28 Dec 1998 09:30:46 -0500

A German couple drove their BMW with great confidence under control of its computerized satellite navigation. Indeed, they drove it past a stop sign, down a ferry ramp, and into the Havel River in Caputh, near Potsdam/Berlin, Germany. The computer system reportedly neglected to tell them they needed to wait for the ferry. Ship traffic was stopped for two hours, but the couple was OK. [Sources: PGN Abstracting from numerous multiply submitted similar copyrighted stories, several quoting different officials reminding us that we should not blindly rely on technology. Big surprise to RISKS readers! But for the price of a Beemer, I thought it drove on water. PGN]

⚡ **Swedish passport system struck by 99**

Ulf Lindqvist <ulfl@ce.chalmers.se>

Fri, 1 Jan 1999 21:51:10 +0100 (MET)

In Sweden, the first report about a 99-related computer problem appeared already on 1 Jan 1999. The Swedish police can normally issue provisional passports at the three main international airports in Sweden. But on the first day of 1999, no passports could be issued because the computer system could not handle 99. Four people in Stockholm and two in Goteborg had to cancel their trips because they could not get their passports. The system was reported to have been fixed during the afternoon. [Primary source *Sveriges Televisions Text-TV*, January 1 1999]

A couple of things to note: Of course it is a risk to try to travel abroad without having a passport, but there could be good reasons - family emergencies, for example. The ordinary Swedish passports where changed in 1998 to conform with European Union regulations, but in this case the system must be much older or based on old components (if the designers where not extremely shortsighted). Most businesses do not open until Monday 4 Jan - we could expect to hear about more 99-problems then, I guess.

Ulf Lindqvist, Department of Computer Eng., Chalmers University of Technology
SE-412 96 Goteborg, SWEDEN +46 31 772 17 60 ulfl@ce.chalmers.se

[Also reported by Martin Minow, and by Debora Weber-Wulff, who notes that 99 seems to be used often in Sweden to denote "end-of-file"... PGN]

⚡ Swedish Giroguide also hit by 99

Martin Minow <minow@apple.com>

Sat, 2 Jan 1999 10:02:39 -0800

The New Year provided an early taste of Y2K in Sweden. According to the Stockholm newspaper, **Svenska Dagbladet**, the modem-based "Giroguide" payment service run by the PostGiro refused to process payments "if the payer provided a specific date in 1999". (PostGiro is a convenient payment system run by the Post Office used as widely as checking accounts in the United States.)

"It was due to a programming error" ... that can depend on the combination "99" that, in some cases, is used to mark end-of-run. Since you can enter payments up to a year in advance, it may also be due to a year-2000 problem, but Jarl Dahlerus, who is responsible for E-PostGiro, doesn't believe this is the case. If any customer is affected by the error, they will be compensated by PostGiro.

Translated and summarized by Martin Minow, minow@pobox.com

⚡ Excel bug

"Tom Rowe" <trowe@ibm.net>

Thu, 31 Dec 1998 23:02:41 +0100

I imagine this has been discussed some, but in case it hasn't. If you enter a number, say 123456789999 in Excel and save the file as comma delimited (csv I think MS uses) it will be saved as 1.234567E+11. Quite a few programs can't import this properly, including Word. But what's worse, bringing it back into Excel gives you 123456700000. I think the risks are fairly obvious. I wonder if the large bank I work for (which has standardized on Excel) knows about it. When opening an account I guess not only do I need to ask banks the interest rates, fees etc, but also what software they use. Sheesh.

Tom Rowe, Atlanta, GA

🔥 Chinese sentence hackers to death

John Knight <jck@cs.virginia.edu>
Thu, 31 Dec 1998 12:38:59 -0500 (EST)

Twin-brother computer hackers sentenced to death in China (Deutsche Presse-Agentur, 28 Dec 1998)

Two Chinese computer hackers who illegally transferred 720,000 yuan (about 87,000 dollars) to their own bank accounts have been sentenced to death, the Beijing Chenbao newspaper said in its Monday edition. The hackers, twin brothers, had used inside information to rob a bank in the city of Zhenjiang, the report said. One of the brothers, Hao Jingwen, opened 16 accounts under false names in September, the report said. Then he entered a branch of the Trade and Industry Bank in Zhenjiang, in Jiangsu province, and

installed a piece of equipment in the bank's computer system.

<http://web.lexis-nexis.com/more/cahners-chicago/11407/4120740/4>

[Extracted from NMIA ZGram, zhi@zgram.net (Zhi Hamby)]

★ Student can criticize school on web site, judge says

Declan McCullagh <declan@well.com>

Tue, 29 Dec 1998 18:02:45 -0500

This case reminds me of another I wrote about earlier this year -- but with a happier ending:

<http://cgi.pathfinder.com/time/digital/daily/0,2822,12983,00.html>

<http://www.wired.com/news/news/politics/story/17068.html>

[Also AP item 28 Dec 1998]

School Dazed by Speech Ruling, by Declan McCullagh

A Missouri high school cannot punish a student for criticizing a teacher on a personal Web page, a federal judge ruled Monday. Saying the school violated free speech rights protected by the First Amendment, District Judge Rodney Sippel ordered the Woodland School District to let the student publish his site from a home computer. "Disliking or being upset by the content of a student's speech is not an acceptable justification for limiting student speech," Sippel wrote in a 17-page opinion.

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/>

🔥 IP: Hackers have fun with Furby (from Robert Raisch)

Dave Farber <farber@cis.upenn.edu>

Sun, 27 Dec 1998 11:05:23 -0500

See Also: Reverse Engineering the LEGO RCX

<http://graphics.stanford.edu/~kekoa/rcx/talk/>

From: "Robert Raisch" <raisch@internautics.com>

(When you provide technically capable, questing minds with simple, cheap and effective communications channels, they do what come naturally. This is why DIVX is doomed. /rr)

Hackers have fun with Furby, BY MARGIE WYLIE, Newhouse News Service

<http://www7.mercurycenter.com/business/top/080145.htm>

Excerpt:

While some people see a lovable little friend in this year's answer to Tickle Me Elmo, toy hackers like the 25-year-old programmer see a challenge: make Furby do as they command. Why? Why not?

``I figured it would be neat,' ' said Tokash, who has created a Web site for Furby hackers to swap information (<http://www.homestead.com/hackfurby>).

``Somebody's going to hack this thing; I might as well be one of them.' '

The Furby was designed by Tiger Electronics of Illinois to

squeal, sneeze or
snore and speak 200 words in a language called Furbish. And
since its
October introduction, hackers have skinned, autopsied and beamed
the
cloyingly sweet animatronic fur-ball with different infrared
signals. The
results, in excruciating detail, are posted on the Web.

Rob Raisch, Internet Technical Hired Gun <<http://www.raisch.com/>>

⚡ Now you see it, now you don't

Jerry Leichter <leichter@lrw.com>

Fri, 25 Dec 98 08:34:22 EST

The Net remembers everything; the Net forgets everything.
What's the effect
on traditional ideas of research?

The Web these days relies on search engines. These are
commercial ventures,
whose distinguishing features are in the technologies used to
implement the
Web crawlers, indexers, and other components. Details of these
technologies
have remained closely guarded trade secrets.

A group at Stanford University set out to do research on some
nice new ideas
for search engines, applying and extending some traditional
ideas from
library science to estimating relevance and importance of
various Web pages.
The algorithms used, the architecture of the system, and other
interesting
stuff, was published as a series of reports, which appeared -
naturally
enough - on the Web at the group's Web site

(<http://google.stanford.edu/about.html>).

If you're interested in learning more ... you're too late. If you go to that site, you'll find that the research group no longer exists. It's been reconstituted as a corporation, Web site <http://www.google.com/company.html>.

That site currently has very little on it. The research papers are no longer on the Web.

Now, I have no objection to the researchers going off to start a company. I wish them the best of luck, even as I worry about the effect the drain of talent from the academic world will ultimately have. However, I am concerned about the removal of previously-public research material. We hear repeated complaints that traditional journals don't accept URL's as bibliographic citations. If *even a university research department* approves the removal of on-line versions of its own research papers, how can we take the Web seriously as a resource for scholarship?

Note that, even if the commercial venture decides to put the papers on-line at its site, that would not be good enough. First of all, if anyone has a citation to the papers at the old cite, the citation should be good on its own - it should not require a chase to another site. More important, however, commercial Web sites come and go. Even with the best of intentions, a commercial Web site is not a stable academic reference. If the new company fails; or if it succeeds, but is acquired by a larger company and disappears as a separate entity; the papers will likely vanish

forever.

[Increasingly, much valuable research from the past is being forgotten.

Unfortunately, the operative motto seems increasingly to be
``If it is not now on the Web, it never existed.'' PGN]

✦ Y1999: Risk of re-using data fields for error signaling

"Daniel A. Graifer" <dgraifer@cais.com>

Wed, 30 Dec 1998 13:12:25 -0500

"1999 problems with medical device clocks found"

<<http://www.sjmercury.com/business/tech/docs/085460.htm>>

discusses two

medical devices that the FDA is warning hospitals of non-health threatening failure in 1999. The HP defibrillator will print "set clock"

instead of the date on its printed record. The other, a patient monitor, will also fail to correctly report the date in it's logs.

Obviously, somebody made "99" mean "clock needs to be reset".

These are

relatively new devices. We they really so short of memory that they

couldn't find a bit somewhere for this flag?

Daniel A. Graifer, Parker & Company 1-888-426-6548

Andrew Davidson & Company, 588 Broadway, Ste 610, NY 10012 1-212-274-9075

[Note: relating to Jerry Leichter's Y2K item in [RISKS-20.13](#), various folks observed that 9 Apr 99 is the 99th day of 1999, which

in some programs is represented as 9999, an erstwhile stopcode. PGN]

⚡ 99-Year retrospective health insurance - or Y2K problem

<Fraser_McHarg@nag.national.com.au>

Tue, 29 Dec 1998 13:40:58 +1000

Last week I received my Health Insurance renewal notice with the period of cover listed as "From: 4 January 1999 To: 4 January 1900". Since I was not alive for most of the 99-year period I am intending to decline their generous retrospective insurance offer.

It does not bode well, that in December 1998, HBA, one of the larger Health Insurance companies in Australia can presumably be so far behind in its Year 2000 project that they have not tested the production of their primary revenue collection document. Many other companies have already finished their Year 2000 projects.

Now is the time that annual renewals for all sorts of things will be issuing that should have expiry dates falling in January 2000, it will be interesting to see how many other 1999 to 1900 renewals appear.

[Many people are actually expecting some serious problems beginning next week for insurance companies and others who have to deal with dates a year ahead. PGN]

⚡ San Francisco power outage and the risks of signs (Horiuchi, R-20.13)

eric leif <REMOVE_ericleif@mindspring.com>

Wed, 23 Dec 1998 03:10:26 -0500

The mention of a pipe and the risk of not having a sign reminded me of an incident. Some background information, this took place in a nuclear training facility. For the most part a "real" plant wouldn't have as many tags and signs as this plant, but every pipe, wire, machine was labeled.

So that's the stage and the pipe in question had the label CPW, the meaning of that pipe was taught early, and everyone there knew what it was, so much in fact that an ongoing joke about its meaning as Coffee Pot Water, however the real meaning of that acronym is Controlled Pure Water. And what that means is this water could be potentially contaminated. Anyway you can probably guess the conclusion of this story, but I will continue anyway. A new trainee, had apparently heard the joke before the lesson, and used CPW to fill up a coffee pot.

The risks here are many. The joke definition of the above incident is really a risk with human nature or boredom of being over trained perhaps, but that aside. The use of acronyms is certainly a risk and I'm sure its been seen on this list many times. Even without using acronyms, the above sign could still be misinterpreted, Controlled Pure Water sounds at first like its pure and guaranteed to be so. Most people at this plant knew what controlled meant in context of this plant, but others? And back to the SF power outage, had that pipe been labeled substation ground, would that have

meant anything
to a construction crew?

The real risk of this power outage would seem to me a physical security risk, as with the CPW incident. Neither of these things needed to be easily accessible, but once they are humans will err.

-eric leif <ericleif@mindspring.com>

⚡ Page-layout program hazards

Jordin Kare <jtkare@ibm.net>
Tue, 29 Dec 1998 10:54:49 -0800

In [RISKS-20.13](#), Ben Sherman <ben@2600.com> noted that Quark Xpress, as part of a "feature" allowing embedded ASCII string commands, would silently convert >> to >, mangling published UNIX listings. This is by no means a new problem, and is, I think, inherent in the use of embedded commands.

Circa 1981, I was typesetting a songbook using TROFF, the UNIX typesetting program in which one flags command lines embedded in text by starting them with a period (.), e.g., .PP signals a new paragraph. After some 2000 copies of the book had been printed and put on sale, we discovered that, in perhaps a dozen places, entire lines of text had vanished. (This is remarkably difficult to detect when proofreading familiar songs, similar to losing complete sentences out of prose text).

On close examination, we found that TROFF had silently "eaten" every line beginning with an apostrophe ('). VERY close reading of the TROFF manual revealed that the apostrophe is an alternate command line marker, so that any line starting with an apostrophe will be treated as a command. This fact was noted in one obscure footnote, and not referenced anywhere else.

Why the programmers thought the apostrophe was a "safe" character to use is unclear, but seems to follow the same logic that caused the Quark Xpress bug: in "normal" writing, one does not use >>, nor start a line with an apostrophe. However, these occur frequently in specific types of writing: in UNIX shell scripts for >>, and in poetry or song lyrics for lines starting with apostrophes (which frequently use contractions like 'Til and 'Tis).

The consistent Risk is that any reserved character combination, no matter how obscure, may occur in someone's text, quite possibly without them realizing it. If there is a solution (other than really careful proofreading of typesetting-program output) it presumably includes conspicuously documenting such combinations, ruthlessly minimizing their number, and trying very hard to avoid anything even remotely likely to be entered other than deliberately.

Jordin Kare

Some new things to try at all.net

Fred Cohen <fc@all.net>

Thu, 24 Dec 1998 17:52:22 -0800 (PST)

Just thought RISKS readers would like to know about a few New Year's gifts from all.net:

I thought many of you might be interested in the newest "game" on <http://all.net/>

The Cracking Game

In this 'game', we teach defenders about attack and defense techniques by having them try to tell us how they would crack into a variety of different sorts of systems and having various defensive things happen to them along the way. It is also a lot of fun and somewhat of a challenge. Just select it from the "Would you like to play a game?" Menu and press Go.

Please note that the game is still under development and your comments will be greatly appreciated.

I have also put up a beta-test version of an automatic game:

The Network Security Simulator

This simulator is intended for design, attack, and defense analysis for computer networks, but it may also be of some interest from a gaming viewpoint. It has just been added to the games menu at <http://all.net/> Just select "Network Security Simulator", select inputs from the menus, press go, and see the results. Press "reload" to simulate again - with different

results of course. Your comments again will be appreciated.

Fred Cohen & Associates: <http://all.net> - fc@all.net - tel/
fax:925-454-0171

[Standard RISKS disclaimer. In this case, FC's work at FC&A
is separate
and independent from any work he does for at Sandia. 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. (For example, vol 13, issue 031, 23 Dec 1998, has a long item on random credit-card fraud via small charges.)

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 20: Issue 15

Sunday 10 January 1999

Contents

- [UAL clock wraparound](#)
[John Rushby](#)
- [Risks of old documentation](#)
[Richard C. Wolber](#)
- [Cell-phone surprise](#)
[Craig DeForest](#)
- [Excel CALL function](#)
[Padgett Peterson](#)
- [Phone service outage when computers stolen](#)
[Peter Kaiser](#)
- [Y2K hits Singapore and Swedish taxi meters](#)
[Keith A Rhodes](#)
- [The Windows April Fools 2001 Bug](#)
[from Richard Smith via Lloyd Wood](#)
- [Editors also mitigate page-layout program hazards](#)
[Glen Turner](#)
- [Re: Now you see it, now you don't](#)
[Jerry Leichter](#)
[Mike Williams](#)
- [Call for Proposals - CFP99](#)

[Marc Rotenberg](#)

● [Info on RISKS \(comp.risks\)](#)

✈ UAL clock wraparound

John Rushby <RUSHBY@csl.sri.com>

Mon 4 Jan 99 23:25:21-PST

I don't know about Y2K, but United airlines has a problem with H24.

This is what www.ual.com provided for the flight status of today's UA63 (scheduled to depart San Francisco at 7:15p and arrive Honolulu at 10:46p)

Flight: UA 0063
Date: 01/04/99

Airport	Time	Status
San Francisco Intl Arpt	9:10pm Mon	Delayed 1 hr 39 min
Honolulu Intl	12:01am Tues	Early 22 hr 35 min

✈ Risks of old documentation

"Wolber, Richard C" <Richard.Wolber@PSS.Boeing.com>

Fri, 8 Jan 1999 12:57:08 -0800

This came from a friend of mine. I dialed the number and it actually works:

```
> I was installing Quickbooks 5.0, dated 1992, for a friend
> Wednesday. We
> had a little trouble, so I thought I would call the 1-800
> support number
> (1-800-INTUIT-7). Well.... I got support all right. A
```

recording of a
> female voice a low, whispering tone starts her sentence with
> "Hi Baby,
> You've just connected with..." I guess Intuit made some extra
> cash by
> selling it's phone number to a phone sex outfit. I wonder, do
> they get
> paid by the minute or number of calls? Needless to say, I did
> feel a
> little better after calling, which motivated me to finally fix
> the problem
> myself. So, everything worked out OK after all

Richard C. Wolber, Software Developer/Troubleshooter
DCAC/MRM Final Assembly G-4865 (425)965-6797

[Your friend almost really got intuit! PGN]

⚡ Cell-phone surprise

Craig DeForest <zowie@urania.nascom.nasa.gov>

Wed, 6 Jan 1999 05:22:19 GMT

A few days ago, I bought a Samsung SPRINT PCS phone at a Radio Shack in Ft. Collins, Colorado. When I pulled it out of the packaging, I noticed that there were some fingerprints on the display window and a scratch on the protective soft-plastic cover (that you're supposed to pull off when you buy the phone). The salesperson laughed and said that it had probably been briefly out of the box for a demo or something. I called Sprint from their wired phone and turned on service, then went home.

Like most new cell phones, this one comes with an online directory.

Unlike most new cell phones, this one had 6 numbers preprogrammed into it:

"Work", "Home", "Cathy", "Lawyer", "Lisa", and "Jess".

I'm not especially upset that I was sold a used phone -- it works just fine.

But it certainly brings to light a general RISK of information appliances:

If you return the appliance, you return the information you've stored in it, too!

I deleted the numbers right away -- but if I'd called "Home" and mentioned

"Jess", "Lisa", and "Cathy", perhaps the "Lawyer" would've gotten some more business...

⚡ Excel CALL function

"Peterson, Padgett" <padgett.peterson@lmco.com>

Fri, 08 Jan 1999 08:52:13 -0500

There is a lot of press being given to this vulnerability (it is NOT a virus

but rather a security "hole"). Data Fellows sums it up best so far:

(<http://www.datafellows.com/v-descs/rnewyear.htm>) .

"This vulnerability, related to the CALL function of Excel, allows an

attacker to send an HTML e-mail or modify a HTML web page so that when

accessed, the HTML page will automatically launch Excel and use that to run

any program. This allows the attacker to do pretty much anything he wants

on the host machine."

What is not well understood is that this exploit is actually multifaceted - there are a number of HTML constructs and a number of applications that can be used. The choke point seems to be in the (Windows) Registry which decides which applications (mostly Microsoft's) are considered "safe", that no warning screen is generated on network download/launch sequences for these applications. EXCEL is just one of these. A similar download sequence can be observed by W98 users when visiting the "Windows Update" page and the check for installed products is made. Note that the download occurs before a screen is displayed..

It would seem that this is necessary for the "Active Desktop" however for over a year various professionals, myself included, have been saying that this concept is flawed and that discovery of intrusion vectors was inevitable. Microsoft has disagreed (but then they disagree with governments also).

One problem is that getting information from the company such as exactly *which* applications are considered "safe" by default is like pulling teeth. The only way at present is to search the Registry as to whether a particular byte in an obscure value is 00 or 01.

As expected Microsoft has announced that there is a fix - but it involves disabling the CALL function entirely, applies to EXCEL97 only (95 responds the same way), and if you do not have the OFFICE service packs installed, be

ready for a 24 Mb download and make sure that there is at least 50 Mb of free disk space afterwards. As usual responding to a symptom and not the cause.

However the root problem is the Registry permissions and the fact that these are either not well documented or not documented at all. As long as these remain, further discoveries are sure to follow.

Padgett Peterson, P.E., Lockheed-Martin Corporate Information Security
1-407.306.1101 padgett.peterson@lmco.com

⚡ Phone service outage when computers stolen

Peter Kaiser <kaiser@acm.org>
Tue, 05 Jan 1999 22:55:14 +0100

On 3 Jan 1999, three men wearing ski masks broke into a Sprint telephone office, tied up workers, shot them with stun guns, and removed live telephone relay switching equipment (perhaps to fill a custom resale order?), knocking out service for about 75,000 customers for about 7 hours.
[Source: Associated Press, 3 Jan 1999, seen in *The Boston Globe* online on 4 Jan 1999; PGN Abstracting.]

This interruption of phone service isn't fundamentally different from utility service disruptions caused by the theft of wiring or pipes. But computers are a lot easier to steal. I believe I reported long ago here on the theft of a computer from an unstaffed area whose exact time

was known
because there were records of exactly when the computer was
taken offline;
but the computer was small enough to fit into an athletic bag,
and was
never found. The thief probably just walked out of the building
with it.

I wonder who buys stolen telephone exchange computers. And what
they say
to the people who service them.

Pete kaiser@acm.org

✶ Y2K hits Singapore and Swedish taxi meters

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

Mon, 04 Jan 1999 10:13:06 -0500

Computerized meters in 300 Singapore taxis failed for about two
hours at
noon on 1 Jan 1999 in an early Y2K manifestation. Taxi meters
in Sweden
also acted up on the same day, but passengers there hardly
complained. The
meters continued to work but gave riders unexpectedly low fares.
[Source: Associated Press, 3 Jan 1999, *The Sunday Times*, PGN
Abstracting]

[NOTE: I guess free parking is one of the new-year's
initiatives that the
government didn't tell people about. Perhaps we can make
certain this
happens in San Francisco, D.C., and New York. The problem of
moving from
1998 to 1999 has also been found in some of the embedded
systems in power
plants, mostly in graphical counters for trend analysis. KR]

⚡ The Windows April Fools 2001 Bug (from Richard Smith)

Lloyd Wood <L.Wood@surrey.ac.uk>
Thu, 7 Jan 1999 13:16:56 +0000 (GMT)

This is really a daylight-savings problem in the Visual C++ library -
but the last time it would have happened would have been in 1990...

More on the webpages. Since it's windows *applications* rather than Windows itself, it can be expected to be widespread.

<L.Wood@surrey.ac.uk>PGP<<http://www.ee.surrey.ac.uk/Personal/L.Wood/>>

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

Date: Thu, 07 Jan 1999 00:39:30 -0500
From: glen mccready <glen@qnx.com>
Subject: The Windows April Fools 2001 Bug [from 0xdeadbeef]

From: "Richard M. Smith" <rms@pharlap.com>

I thought the deadbeef crowd might be interested in this story.....

I just got confirmation from Microsoft of the "April Fools 2001" bug that I reported on Monday. Although not technically a Y2K bug, many Windows applications are going to break on April 1, 2001 and start giving the wrong time of day. The bug lasts for a week.

Technical details of the bug can be found at:

<http://security.pharlap.com/y2k/aprill1.htm>

A live test page for the bug is available at:

<http://security.pharlap.com/y2k/demo1.htm>

With this bug, any technical person involved with Y2K testing has a new date to worry about which April 1, 2001.

Richard

✶ Editors also mitigate page-layout program hazards

Glen Turner <glen.turner@adelaide.edu.au>

Thu, 07 Jan 1999 01:02:17 +1030

In [RISKS-20.14](#) Jordin Kare <jtkare@ibm.net> gives a number of sensible methods to decrease the risk of not noticing the delimiting characters used to separate text from page layout commands.

A most useful method is not mentioned -- use an editor that displays differing syntactic components using differing textual properties.

This makes the difference between text and markup commands much clearer. A good editor will also highlight common syntactic errors.

Such editors date from at least the Andrew project. I recall the facility being available in 1984 for Pascal when I used DEC's LSE editor running on the VMS operating system.

These days, I happen to use the XEmacs editor and the Linux operating system. To take Mr Kare's concrete problem, text in TROFF source appears in

a black normal-weight font. TROFF commands, whether indicated by an apostrophe or other characters, appear in a green bold-weight font. Text and markup are much less readily confused.

Glen Turner. Network specialist, The University of Adelaide.

⚡ Re: Now you see it, now you don't ([RISKS-20.14](#))

Jerry Leichter <leichter@lrw.com>

Fri, 8 Jan 99 20:01:27 EST

> [Increasingly, much valuable research from the past is being forgotten.
> Unfortunately, the operative motto seems increasingly to be
> ``If it is not now on the Web, it never existed.'' PGN]

Well ... there's more to it than that.

Computer science is unique in its reliance on non-traditional means of publication. There's been an over-reliance on conferences and conference proceedings, which are not handled well by libraries. Further, while conference papers are peer-reviewed, the level of review - and the consequent level of the papers - has never matched what you get in the traditional publication venues. There are exceptions - SOSP, to cite one example, has tended to have unusually good papers - but by and large a conference paper is a good first draft for a journal paper (but most never appear in journals). Things have historically been even worse in CS theory, where often all you find in the conference proceedings is an

extended
abstract - and the final paper somehow never gets published.

The other over-reliance has been on technical reports. Some technical report series are excellent - I've got a pile of old PARC reports that are wonderful; many of the MIT reports were great when I was looking at them. Most tech report series are of very variable quality, however - and of course you can't find *them* either.

All of this was the case before the Web came along. It all of a sudden appeared to be the solution to the CS publications problem. Just put all the tech reports and whatever on-line, and they'll be available to everyone everywhere. Except that (a) they disappear anyway; (b) the quality is extremely variable.

I've been out of academia for over 3 years now, and I let my ACM and IEEE memberships lapse - the stuff was piling up way faster than I could find time to read it, between a non-academic job and an infant (now youngster). I do follow papers in a number of areas, and indeed they are much more accessible now than they used to be. But serious research - in the sense of finding the work already done in a field - can be tricky. Stuff is unorganized, un-reviewed, of unpredictable quality - and it disappears.

Then again, we don't respect the history of our own field. Books go out of print rapidly - and libraries can't keep up. I collect the classics when I can get my hands on them; they're irreplaceable, and often still

valuable.

(I'm also always amazed by the quality of writing of papers from the 60's and early '70's. We've lost that.)

We like to think that we in CS are on the leading edge of a revolution, but the fact is **it** is driving **us**. Things are different in other fields.

Physicists have done a much better job of integrating the Internet and the Web with their research and publications. It helps to have an established way of working, not just make everything up on the fly. (And, of course, it was the physicists - not us CS types - who invented the Web.)

Jerry

✉ Re: Now you see it, now you don't (Leichter, [RISKS-20.14](#))

Mike <John.Michael.Williams@Computer.org>

Fri, 08 Jan 1999 18:59:05 -0500

Is it still on the web if it's locked down? ACM used to have the ACM

Turing Award Lectures, including Ken Thompson's classic, seminal "Reflections on Trusting Trust," on the web available at no charge.

Now, as an ACM member since '64, I have to pay a high premium to get it, or to pass it on others who need it more than they know.

Fat chance.

Mike Williams

Call for Proposals - CFP99

Marc Rotenberg <rotenberg@epic.org>

Tue, 5 Jan 1999 17:26:32 -0500

[I could have titled this CFP for CFP99, but that would be confusing. PGN]

Computers, Freedom + Privacy 1999
THE GLOBAL INTERNET
Omni Shoreham Hotel
Washington, DC
April 6-8, 1999

The Program Committee of the conference on Computers, Freedom, and Privacy (CFP99) is seeking proposals for the ninth annual CFP, which will be held in Washington DC between April 6th and April 8th 1999 at the Omni Sheraton Hotel. CFP is the leading Internet policy conference. For almost a decade, CFP has shaped the public debate on the future of privacy and freedom in the online world. The CFP audience is diverse with representatives from government, business, education, non-profits and the media. The themes are broad and forward-looking. CFP explores what will be, not what has been. It is the place where the future is mapped.

The theme of the 1999 CFP conference is "The Global Internet." Proposals are welcomed on all aspects of privacy and freedom. The 1999 Program Committee is particularly interested in receiving proposals that deal with:

ACCESS TO THE INTERNET, particularly those relating to globalization and governance. Of particular interest are issues of privacy, censorship, free speech and access.

INTERNATIONAL ISSUES, especially the emerging issues of global privacy protection, encryption policy, international principles of human rights, regulation, legislation, and copyright.

ELECTRONIC COMMERCE, including the impact of payment systems, regulations, and technical standards on personal freedom and privacy.

CULTURE AND LANGUAGE ON THE INTERNET, such as the significance of diversity, multilingualism, and cultural representation

We strongly encourage proposals that involve leading experts, innovators, policymakers, and thinkers. The CFP99 Program Committee will finalize the selection of proposals by February 1, 1999, proposals should be received by 15 Jan 1999 by e-mail to proposals@cfp99.org [Apparently, slightly late proposals will be considered if they are good, which is why I am running this notice on 15 Jan 1999! PGN]

For more information on the Computers, Freedom, and Privacy Conferences, please visit the conference Web page <http://www.cfp99.org>. If you have further questions about CFP, please feel free to contact a member of the Program Committee.

PROGRAM COMMITTEE chair: Marc Rotenberg, EPIC and ACM, Washington, DC.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 16

Friday 15 January 1999

Contents

- [Another premature data release](#)
[PGN](#)
- [NSA says Furby is a national security risk](#)
[Bruce Martin](#)
- [Man crashes car as 50 pagers ring simultaneously](#)
[Geoffrey Leeming](#)
- [16-yr-old Irish girl's crypto system](#)
[PGN](#)
- [Over-reliance on technology](#)
[Pat Place](#)
- [The risks of a first failure](#)
[Bertrand Meyer](#)
- [If at first you don't succeed, breaking-in's no crime in Norway](#)
[Edupage](#)
- [Viruses and Rocket Science](#)
[Henry Spencer via Tom Evans](#)
- [Smurf denial-of-service attack on OZEMAIL](#)
[Mich Kabay](#)
- [Y2K in Swiss hospitals](#)
[Debora Weber-Wulff](#)

- [1 Apr 2001 flaw in Windows](#)
[PGN](#)
 - [Quicken 1999 bug](#)
[James S. Vera](#)
 - [A good Y2K bug](#)
[Lenny Foner](#)
 - [Utilities and Y2K: not to worry](#)
[Ken Knowlton](#)
 - [Y2K testing tools](#)
[Craig Raskin](#)
 - [Java Security](#)
[Gary McGraw](#)
 - [REVIEW: "Maximum Security", Anonymous](#)
[Rob Slade](#)
 - [REVIEW: "Year 2000 in a Nutshell", Norman Shakespeare](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ Another premature data release

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

Tue, 13 Jan 1999 08:12:17 -0800 PST

The Department of Labor Statistics has once again accidentally released data a day early, this time with the Producer Price Index. Whereas last time ([RISKS-20.05](#)) it was "a human failure", this time it was attributed to a ``software programming error''. As usual, the problem has been corrected, and won't happen again. [Source: *San Francisco Chronicle*, 13 Jan 1999, front page of the business section, PGN Abstr.]

🔥 NSA says Furby is a national security risk

<Bruce_Martin@manulife.com>

Wed, 13 Jan 1999 13:15:00 -0500

On 13 Jan 1999, CNews (www.canoe.ca) carried the AP news story about a U.S.

national security risk posed by the stuffed toy sold under the name of

Furby. For the uninitiated, Furby was the hottest-selling toy of the Xmas

'98 season. Resembling furry gremlins [and apparently being sued therefor],

Furbies are bristling with audio, infrared, and touch sensors, allowing them

to interact with people and with others of their kind.

Detailed information on the capabilities (intended or not) of the average

Furby can be found at: www.homestead.com/hackfurby. Among their repertoire

of tricks, these toys have the apparent ability to mimic human speech in

parrot-like fashion, and therein lies the risk.

According to no lesser authority than the National Security Agency, these

toys were being brought into top-secret areas at Fort Meade by government

employees, where the little devils (the toys, not the employees) could

easily be exposed to classified information which they might later repeat

to foreign agents.

Furby is now "machina non grata" at Fort Meade, and transgressors are to

report to their Staff Security Office for guidance on this matter. A Capitol

Hill source is quoted in the Washington Post of 13 Jan 1999 as

saying they
feared "that people would take them home and they'd start talking
classified."

The risk of U.S. national security resting in the hands of
adults who play
with children's toys during office hours is left as an exercise
to the
reader.

Bruce Martin, Toronto

[The manufacturer insists that the memory cannot be altered,
and

that the furbies cannot learn from their environments.

However,

because Furbies are programmed to react to responses, there is
always the

question of whether there might be a preprogrammed Trojan
horse recording

their choices, and providing a nifty covert channel. Until
recently, if

you brought viewgraph transparencies into the agency to give a
talk, it

was nontrivial to get them out again -- because they were
photographic

media. Presumably, similar thinking goes into NSA's Furby
policy. PGN]

⚡ Man crashes car as 50 pagers ring simultaneously

<geoffrey.leeming@henderson.com>

Fri, 15 Jan 1999 11:27:39 -0100

A man in the Ukraine bought 50 pagers as presents for his
staff. While
driving home, they all rang at the same time. He was so
distracted that he
crashed into a lamp post, within 100 meters of his office. Of

course,
each one said simply, ``Congratulations on a successful
purchase!''
[Source: Yahoo News via Reuters, 15 Jan 1999; PGN Abstr.]

✶16-yr-old Irish girl's crypto system

"Peter G. Neumann" <Neumann@csl.sri.com>
Wed, 13 Jan 1999 08:20:21 -0800 PST

Sarah Flannery, 16, in Blarney, County Cork, Ireland, has
designed a crypto
system (called Cayley-Purser). ``She is considering publishing
her findings
rather than patenting as she does not want people to pay for her
discovery.''
Source: Audrey Magee, *The Times*, London, 13 Jan
1999;
Edupage, 14 January 1999, PGN Stark Abstr. TNX to Lindsay
Marshall]

According to some technical discussions on the net, the scheme
is based on
2x2 matrices, and appears to be 10 times faster than RSA, but
with much
longer keys, and apparently with security comparable to RSA
for comparable
modulus sizes.

I'm not sure from the articles I've seen whether the
reporters are
more surprised by Sarah's age or her gender. But there
seems to be
general astonishment that she could come up with a crypto
algorithm. On
the other hand, RISKS readers know that lots of people have
come up with
crypto algorithms. If this one is really good, that *is*
special.

That she wants to keep it open is even more special. PGN

✂ Over-reliance on technology

Pat Place <prp@SEI.CMU.EDU>

Tue, 12 Jan 1999 09:07:19 -0500

In answer to Jordin Kare's TROFF problems ([RISKS-20.14](#)), Glen Turner ([RISKS-20.15](#)) suggests the use of a text editor displaying different syntactic components using different textual properties (colour, font, and size being the common variables).

I'm sure that XEmacs and other editors of that sort do their best, however, with a language such as TROFF, where everything can be changed including the escape character and the control line characters (.ec, .cc, and .c2), unless the editor contains a TROFF interpreter sooner or later it will be confused.

Although, XEmacs' best attempt may be good - we shouldn't rely on it for accuracy - the best solutions to Jordin Kare's problems are

- 1) understand the tool you are using (the nroff/troff user manual is invaluable here)
- 2) proof-read carefully everything you produce.

Pat Place prp@sei.cmu.edu

✂ The risks of a first failure

<Bertrand.Meyer@eiffel.com>

Wed, 13 Jan 99 11:14:53 PST

A cute little bug on <http://www.dejanews.com> (but please don't try this except possibly on a test group):

Successfully post an article through DejaNews (after registering as a user)

You get an article number <nnnn> to be used if you want to cancel

Change your mind (L'uomo e` mobile)

Go to the cancellation page, include nnnn as the article number

(You are not only fickle but careless, and didn't notice

that you are supposed to put in the angle brackets too.)

It finds your article

Confirm cancellation by clicking the appropriate button

You get a message stating that this is not a valid article number

Realize your mistake (the forgotten angle brackets)

Try cancellation again, this time including the brackets

It finds your article

Confirm cancellation

You get a message to the effect that this article appears to have been

cancelled already!

As far as I know there is no way after that to cancel the article (but I haven't contacted Dejanews about it).

The reason I mention this small apparent bug is that it is representative of

an interactive system risk that one encounters all too frequently. It arises

for a kind of "transaction", in the broad sense of the term, that a system

accepts to carry out at most once. If, however, an attempt fails and is

rejected by the system, it may have been registered in the same way as a

successful attempt, so that later on the system may believe that

the transaction has already taken place, and reject any further attempt, resulting for the user in a Catch-22 situation.

The more general design principle is: if you reject an operation after it may already have affected the information in your system, make sure that the rejection process brings the information back to a consistent state.

(I am not writing: "... that it restores the information to its original

state", because that may be impossible; even if possible it may be

undesirable, e.g. we may want to keep a record of failed attempts. What we

don't want is partial success leading to an inconsistent database.

Obviously the use of invariants and other Design by Contract principles

helps in defining and enforcing "consistent" states.)

People designing transaction processing systems in the strict, conventional sense are well aware of the risk and the principle, but I think we would all benefit if it were known and applied much more broadly.

Bertrand Meyer, Interactive Software Engineering, Santa Barbara
<Bertrand.Meyer@eiffel.com>, <http://eiffel.com>

✶ If at first you don't succeed, breaking-in's no crime in Norway

Edupage Editors <edupage@franklin.oit.unc.edu>

Thu, 14 Jan 1999 11:52:05 -0500

The Supreme Court in Norway has ruled that it's not a crime to try to break into someone else's computer system, because people should expect others to try to invade their systems, and take measures to protect themselves. There is a crime, ruled the court, only if the system is actually breached. The case developed out of an attempt by a computer security company to break into the University of Oslo's computers through the Internet, to contribute to a feature story by the Norwegian state broadcasting network. Apparently the security company mapped holes in the university's computer security, but did not break in, tamper with, or steal any information. (*USA Today*, 13 Jan 1999; Edupage, 14 January 1999)

⚡ Viruses and Rocket Science

Tom Evans <TEvans@tennyson.com.au>

Fri, 15 Jan 1999 19:03:18 +1100

The following is lifted directly from Henry Spencer's summary of AW&ST posted to sci.space.news:

Date: 1999/01/06

>From: Henry Spencer <henry@spsystems.net>

Subject: space news from Nov 16 AW&ST

As if Sea Launch didn't have trouble enough, now its computers (as well as those of some other Boeing projects) have come down with a massive virus infection. The viruses apparently spread via documents about Sea Launch

export compliance, which were widely distributed to staff in the wake of the project's recent government problems. Boeing had few defences in place, and was slow to act because the viruses initially seemed harmless.

Full article available as:

[http://x7.dejanews.com/getdoc.xp?
AN=429551406.1&CONTEXT=916023969.559415504&
hitnum=1](http://x7.dejanews.com/getdoc.xp?AN=429551406.1&CONTEXT=916023969.559415504&hitnum=1)

Tom Evans <TEvans@tennyson.com.au>

✶ Smurf denial-of-service attack on OZEMAIL

Mich Kabay <mkabay@compuserve.com>

Thu, 14 Jan 1999 09:47:48 -0500

According to an article by Tim Barlass in the Daily Telegraph of Australia (12 Jan 1999, p. 9), someone has launched a sustained smurf denial-of-service attack on Ozemail, an important Australian Internet service provider. E-mail service has been disrupted for users in Sydney. A company spokesperson said they were trying to track down the perpetrator and were considering installing filtering software to prevent future attacks.

[Note from MK: a "smurf" attack uses widely-available software written by

criminal hackers to send ping packets with forged origination in the

headers to a (usually major) corporate network's broadcast address. Every

device -- perhaps hundreds or thousands -- sends a reply

packet to the

forged originator address. That system thus receives a flood of packets,

often overloading its TCP/IP stacks and resulting in denial of service.

See the article by Michael Dillon in ASK THE INFRA EXPERT (Internet World:

Apr 20, 1998) for a more detailed explanation.]

M. E. Kabay, PhD, CISSP / Director of Education
ICSA, Inc. <<http://www.icsa.net>>

✶ Y2K in Swiss hospitals

Debora Weber-Wulff <weberwu@tfh-berlin.de>

Thu, 14 Jan 1999 14:22:58 +0100

I heard about this from an informant, took quite some searching to find the little notice hiding on the pages in the NZZ (Neue Zuercher Zeitung, 7 Jan 1999) usually reserved for reporting celebrity divorces, plane crashes and natural disasters. An on-the-fly translation:

The hospitals in the canton de Vaud (Waadt) spent the 1st and 2nd of January 1999 fighting with the computer problems that are expected for the year 2000. Except for the University Hospital in Lausanne, the computer systems for admitting patients in all of the hospitals of the canton were down for 36 hours. Specialists were able to fix the problem, according to a spokeswoman for the hospitals in the newspaper "24 Heures" (24 hours) on Wednesday. The reason for the system crash is the fact that it

was
programmed to compare something with the date a year in the
future. This
was programmed in 6 digits as "01.01.00". The system
interpreted this as 1
Jan 1900. Source: Year-2000 computer problem in Waadtlaender
hospitals
Lausanne, <http://archiv.nzz.ch/books/nzzmonat/0/8466081T.html>]

Prof. Dr. Debora Weber-Wulff, Technische Fachhochschule Berlin
FB Informatik, 13353 Berlin, Germany <http://www.tfh-berlin.de/~weberwu/>

[Waadt's New? PGN]

[Canton Waadt is known elsewhere as Canton de Vaud.

Correction inserted later in archive copy, suggested by
Bertand Meyer,

who also suggested an additional pun:

"Vaud denn ist dieser Kanton?"

Thanks! PGN]

✶ 1 Apr 2001 flaw in Windows

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

Thu, 14 Jan 1999 18:12:12 -0800 PST

Windows (95,98,NT) systems apparently suffer from an off-by-one-
week glitch

on the daylight savings time cutover in 2001, shifting on 1 Apr
rather than

8 Apr. An updated library program will solve the problem.

[Source: John

Markoff, *The New York Times*, 14 Jan 1999; PGN Abstr, via Dave
Farber and
others.]

⚡ Quicken 1999 bug

"James S. Vera" <vera@anna.stanford.edu>

Tue, 12 Jan 1999 16:44:39 -0800

Another 1999 bug, Intuit's Quicken'99 fails with a "divide by zero" message when a transaction dated in January 1999 is recorded in the Auto category and its "Home and Car Center" is opened. See <http://www.intuit.com/support/quicken/faqs/win2/1913.html>

James S. Vera		Internet		Voice:
+1.415.725.0256				
Stanford University		vera@anna.stanford.edu		FAX:
+1.415.725.7398				

⚡ A good Y2K bug

Lenny Foner <foner@media.mit.edu>

Wed, 13 Jan 1999 01:59:00 -0500

> January 1, 2000
> Re: Vacation Pay

> Dear Valued Employee:

> Our records indicate that you have not used any vacation time over the
> past 100 year(s). As I'm sure you are aware, employees are granted 3
> weeks of paid leave per year or pay in lieu of time off. One additional
> week is granted for every 5 years of service.

> Please either take 9,400 days off work or notify our office

and your next

> pay cheque will reflect payment of \$8,277,432.22 which will include all

> pay and interest for the past 1,200 months.

> Sincerely, Automated Payroll Processing

⚡ Utilities and Y2K: not to worry

Ken Knowlton <KCKnowlton@aol.com>

Mon, 11 Jan 1999 20:49:06 EST

I quote from a 10 Jan 1999 article in *The Boston Globe* on utilities' Y2K readiness:

Typical is one filing from Northeast Utilities: "NU has found nothing

that cannot be repaired or replaced and be made Year 2000 ready in time,"

it states.

They don't get it: the devil is in the gotchas not found.

⚡ Y2K testing tools

Craig Raskin <raskin@compusec.org>

Wed, 13 Jan 1999 14:58:28 -0500 (EST)

I am currently involved with doing y2k testing at a client site.

I have

spent numerous hours looking for tools which can be used for building test

suites. Unfortunately, I have not been able to find very many

tools which
are worthwhile.

A lot of the available tools appear to have been built by individuals who do not fully grasp the underlying concept of the machines and operating systems which they are trying to test.

I have written some c code which should cause alerts with testing software that checks for possible y2k problems. When compiled and checked under microsoft based platforms, these binaries easily slip by testing programs. When compiled and checked by Sun's own y2k testing tools, these binaries also slip by.

Since Sun's tools are based on shell scripts, I was able to go in and find the problem. The script works fine under the Sparc editions of the operating system but returns false information when run under the Intel x86 version. This is due to the 'dump' command having differing output between the OS versions. This slipped by the engineers at Sun.

Out of necessity, a lot of people are now doing system testing for the first time in their careers. The risks are obvious. How many systems have been checked and certified with buggy tools? Have individuals involved with testing first checked that their test suites will actually work? Do they even know how? We will find out soon enough.

Java Security

Gary McGraw <gem@rstcorp.com>

Wed, 13 Jan 1999 22:35:54 -0500 (EST)

Ed Felten and I are pleased to announce the publication of a completely revised and expanded new book, a follow-on to our original 1996 book "Java Security: Hostile Applets, Holes, and Antidotes" (better known as Java Security HA HA among readers in the know). The new book "Securing Java: Getting down to business with mobile code" is published by John Wiley & Sons (1999). Physical copies are available now. In addition to the physical book, Ed and I decided to make the entire text available for free and unlimited Web access. The URL is:

<http://www.securingjava.com>

The risk here is that nobody will buy the physical edition ;-)! Help us mitigate that risk, making the Web experiment a success. Ah publishing in the 90s.

The book covers the risks presented by mobile code systems including Java 2 and ActiveX and is an in depth treatment of these complex issues. RISKS readers will probably appreciate the tone.

Enjoy!

Dr. Gary McGraw, Vice President, Reliable Software Technologies
<http://www.rstcorp.com>

✶ REVIEW: "Maximum Security", Anonymous

"Rob Slade, doting grandpa of Ryan and Trevor" <rslade@sprint.ca>

Mon, 11 Jan 1999 09:59:59 -0800

BKMAXSEC.RVW 981025

"Maximum Security", Anonymous, 1998, 0-672-31341-3,
U\$49.99/C\$70.95/UK#46.95

%A Anonymous

%C 201 W. 103rd Street, Indianapolis, IN 46290

%D 1998

%E Mark Taber newtech_mgr@sams.mcp.com

%G 0-672-31341-3

%I Macmillan Computer Publishing (MCP)

%O U\$49.99/C\$70.95/UK#46.95 800-858-7674 <http://www.mcp.com>

%P 829 p. + CD-ROM

%T "Maximum Security, second edition"

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 first edition

of the book. The introduction to that edition made it fairly clear:

Anonymous assumed that if you did not work diligently at his direction you

did not deserve to secure your system. One could almost feel

his glee at
the expectation that thousands of sysadmins around the world
were wracking
their brains and flooding Usenet with discussions of the
significance of his
clues to the vital encrypted message he had hidden on the CD-ROM.

The riddle, and that attitude, seem to have been removed from
this second
edition. The author tacitly admits that the first was a bit of
a kludge: he
says that it was written in haste. He also states that the
second edition
is more "solution oriented." It could hardly have been less.
Be that as it
may, the book is, as the author states, essentially completely
rewritten.
It has been much improved in the process, moving up from truly
awful to
merely mediocre. The new version provides a good deal of
reference
information, although assessing the quality of that information
is left as
an exercise to the reader.

The section on viruses is an overview of the book in miniature.
The hype
has been toned down, and the explanation of how viruses work is
much more
reasonable. However, it still insists that "destruction" is the
major
characteristic of a virus. (There is, later, an admission that
"[m]ost
viruses do not actually destroy data.") We are treated to the
old myth that
virus researchers write viruses as a kind of job security.
While a general
background to viruses is provided, there is no discussion of
protection
options. However, there are more listings of antiviral programs
and
resource sites than there are for virus creation programs. Many
topics

within the text have lists of books and Web sites for further study, and there is one for viruses that includes three of the four tomes recommended by the VIRUS-L FAQ. Unfortunately, it also contains some lesser works, and there are no annotations to the bibliography.

Part one is simply two chapters of introduction to the book. A somewhat limited overview to security concepts is given in part two, concentrating on the Internet. Chapters look at the Internet, TCP/IP basics, hackers and crackers, targets, possibilities of fights over the net, and very brief data security primer. Various types of security and attack software are outlined in part three. There is consideration of malicious software, weakness scanners, password crackers, trojans, network packet sniffers, firewalls, and audit software. Part four looks at specific operating systems: Windows, UNIX, Novell, VMS, and Macintosh. Two chapters look at very basic security requirements in part five. Network based attacks are discussed in part six, reviewing levels of attack, spoofing, telnet, scripting languages and extensions, and hiding of identity. Different types of resources and references are contained in appendices. (I was disappointed in the loss of a chapter on laws in various countries until I found it had been moved back here.)

If you don't know security, this book is probably not going to teach it to you. On the other hand, if you work with security, you may find that some of the resources listed here are things that you want to explore. For the

novice it isn't altogether reliable, but for the professional it is at least worth looking at.

copyright Robert M. Slade, 1998 BKMAXSEC.RVW 981025
rslade@vcn.bc.ca rslade@sprint.ca robertslade@usa.net
pl@canada.com

Robert Slade's Guide to Computer Viruses, 0-387-94663-2 (800-SPRINGER)

REVIEW: "Year 2000 in a Nutshell", Norman Shakespeare

"Rob Slade, doting grandpa of Ryan and Trevor" <rslade@sprint.ca>

Fri, 15 Jan 1999 08:18:30 -0800

BKY2KNSH.RVW 981030

"Year 2000 in a Nutshell", Norman Shakespeare, 1998, 1-56592-421-5,

U\$19.95/C\$29.95

%A Norman Shakespeare

%C 103 Morris Street, Suite A, Sebastopol, CA 95472

%D 1998

%G 1-56592-421-5

%I O'Reilly & Associates, Inc.

%O U\$19.95/C\$29.95 800-998-9938 707-829-0515 nuts@ora.com

%P 336 p.

%T "Year 2000 in a Nutshell: A Desktop Quick Reference"

Can the Year 2000 problem be put in a nutshell? (Please?)

And isn't it just a tad late to be starting this? (On the other hand,

Nutshell books *are* generally worth waiting for.)

Part one is a general overview of the situation. Chapter one starts with a rather exaggerated doomsday scenario, including concerns that have already

been seen, and thus have been addressed. At the same time, it ignores the "upstream" multiplier effect of supplier and infrastructure failures. However, it does go on to note needs and concerns for management of the potential failures. Management and budgeting considerations are expanded in chapter two. Legal questions are addressed in chapter three, in a somewhat generic fashion. Some standard planning models and assumptions are given in chapter four. A little technical information in chapter five may help with calculations for dates and windowing or packing solutions. Chapter six looks at the desktop PC; which is interesting in view of a very heavy COBOL and IBM mainframe and mid-range emphasis elsewhere (as well as a few PC related goofs in the doomsday scenario). Unfortunately, some of the information is missing and some is wrong in regard to the desktop. There is no mention of a "cold rollover" test for the CMOS/system date, and the statement about Excel's date interpretation is incorrect. (I have confirmed this in my own testing.) On the other hand, the warning about internally developed applications is quite important.

Part two provides some forms and checklists to help organize a Year 2000 project, including triage, inventory, and a project template. There are about a hundred pages of COBOL references and tutorial in part three. Date functions get extensive listings in part four with attention to general types, COBOL, PL/1, MVS LE, Visual Basic, and C. There is a conceptual look at code scanners in chapters eighteen and nineteen. An appendix

lists Web sites for Y2K vendors, tools, and other resources.

Was it worth waiting for this? I'm not sure. There is little wrong with the information, but neither is this a cut and dried quick fix that you might expect from the Nutshell series. An unrealistic expectation in the case of the disaster of the century, admittedly, but there you are. Still, with the big iron emphasis, and the big project orientation, the material is this work seems to be coming later than it would have been necessary to start these kinds of projects. There is relatively little in the volume for small businesses depending upon desktop machines, and almost nothing on fallback plans for non-compliance in the supply chain. The material is fine as far as it goes, but it doesn't go as far as it needs to at this late date.

On the other hand, it's no worse than any of the others.

copyright Robert M. Slade, 1998 BKY2KNSH.RVW 981030
rslade@vcn.bc.ca rslade@sprint.ca robertslade@usa.net
pl@canada.com

Find virus, book info <http://victoria.tc.ca/int-grps/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 20: Issue 17

Weds 20 January 1999

Contents

- [Remarkable French announcement on crypto policy](#)
[Enzo Michalangeli and John Young via Steve Bellovin from cryptography newsgroup](#)
 - [Deep Crack cracks RSA's DES challenge in less than one day](#)
[PGN](#)
 - [The RISKS of Web links](#)
[Daniel R. Tobias](#)
 - [Virginia online sex offender database](#)
[Joe Thompson](#)
 - [China solves the Millennium bug](#)
[Pete Mellor](#)
 - [Computer crash blew up radio listener's request messages](#)
[Kenji Rikitake](#)
 - [REVIEW: "Stopping Spam", Alan Schwartz/Simson Garfinkel](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Remarkable French announcement on crypto policy

Steve Bellovin <smb@research.att.com>

Tue, 19 Jan 1999 17:59:22 -0800

Date: Wed, 20 Jan 1999 08:50:53 +0800
From: "Enzo Michelangeli" <em@who.net>
To: "John Young" <jya@pipeline.com>, <cryptography@c2.net>
Subject: Re: France allows 128-bit crypto

The third legislative initiative concerns cryptography. With the development of electronic espionage instruments, cryptography appears as an essential instrument of privacy protection.

We had, one year ago, made a first step towards liberalization of cryptographic instruments. At that time I had announced that we were going to make one further. The Government has, since then, heard the players, questioned the experts and consulted its international partners. We have today become convinced that the legislation of 1996 is no longer suitable. In fact, it strongly restricts the usage of cryptography in France, on the other hand, for all that, without allowing the public powers to fight effectively against criminal actions of which encryption could facilitate the dissimulation.

In order to change the orientation of our legislation, the Government has thus retained the following orientations, that I have discussed with the President of the Republic:

- - To offer a complete freedom of use of cryptography
- - To remove the compulsory nature or third-party escrow of encryption keys
- - To supplement the current legal framework by the introduction of

obligations, together with penal sanctions, concerning the handing-over

to the legal authorities, when they require it, of the cleartext version of encrypted documents. At the same time, the technical skills of the public authorities will be significantly improved.

Changing the law will take many months. The Government has decided that the main obstacles holding up the citizens from protecting the

confidentiality of their communications and the development of electronic commerce be lifted without waiting. Also, waiting for the announced legislative changes, the Government has decided to raise the the the threshold of cryptology the use of which is free, from 40 bit to 128 bit, considered by the experts a level suitable to ensure durably a very high security.

- - -

Time to sing the Marseillaise again? :-)

Enzo

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

From: John Young <jya@pipeline.com>

To: cryptography@c2.net <cryptography@c2.net>

Date: Wednesday, January 20, 1999 7:11 AM

Subject: France Allows 128 Bit Crypto

The French Prime Minister today announced that due to the threat of espionage and invasion of privacy France will allow encryption strength up to 128 bits:

<http://www.premier-ministre.gouv.fr/PM/D190199.HTM>

(c) Le troisième chantier législatif concerne la cryptologie. Alors que se développent les moyens d'espionnage électronique, la cryptologie apparaît comme un moyen essentiel pour protéger la confidentialité des échanges et la protection de la vie privée.

Nous avons, il y a un an, franchi un premier pas vers la libéralisation des moyens de cryptologie. J'avais annoncé alors que nous en franchirions un autre ultérieurement. Le Gouvernement a,

depuis, entendu les acteurs, interrogé les experts et consulté ses partenaires internationaux. Nous avons aujourd'hui acquis la conviction que la législation de 1996 n'est plus adaptée. En effet, elle restreint fortement l'usage de la cryptologie en France, sans d'ailleurs permettre pour autant aux pouvoirs publics de lutter efficacement contre des agissements criminels dont le chiffrement pourrait faciliter la dissimulation.

Pour changer l'orientation de notre législation, le Gouvernement a donc retenu les orientations suivantes dont je me suis entretenu avec le Président de la République :

- - offrir une liberté complète dans l'utilisation de la cryptologie ;
- - supprimer le caractère obligatoire du recours au tiers de confiance pour le dépôt des clefs de chiffrement ;
- - compléter le dispositif juridique actuel par l'instauration d'obligations, assorties de sanctions pénales, concernant la remise aux autorités judiciaires, lorsque celles-ci la demandent, de la transcription en clair des documents chiffrés. De même, les capacités techniques des pouvoirs publics seront significativement renforcées.

Changer la loi prendra plusieurs mois. Le Gouvernement a voulu que les principales entraves qui pèsent sur les citoyens pour protéger la confidentialité de leurs échanges et sur le développement du commerce électronique soient levées sans attendre. Ainsi, dans l'attente des modifications législatives annoncées, le Gouvernement a décidé de relever le seuil de la cryptologie dont l'utilisation est libre, de

40 bits à 128 bits, niveau considéré par les experts comme
assurant
durablement une très grande sécurité.

⚡ Deep Crack cracks RSA's DES challenge in less than one day

Neumann@CSL.sri.com <"Peter G. Neumann">

Wed, 20 Jan 1999 11:00:17 PST

On Monday morning around 9am when this year's RSA DES challenge
was

announced by Jim Bidzos at this week's RSA Data Security
Conference in San

Jose, John Gilmore set Deep Crack to work. (See [RISKS-19.87](#) for
background.) About 22:25 hours later, Deep Crack had found the
56-bit DES

key, capturing the \$10,000 prize by breaking the 24-hour mark.

This latest

event further dramatizes the inherent risks of relying on
cryptography.

(In three hours, Matt Blaze, Steve Bellovin, and I (with Jeff
Schiller

unfortunately in absentia) tackle the question "Is Cryptography
Enough?"

RISKS readers know well that the answer is NO.)

⚡ The RISKS of Web links

"Daniel R. Tobias" <dan@softdisk.com>

Sat, 16 Jan 1999 11:20:21 -0600

I received a message this morning from somebody complaining
about my

inclusion of a link to a pornographic Web site from a page that
would

otherwise have been a suitable resource for him to refer to

scholars and students interested in the topic of my page. This came as news to me, as I had no knowledge of having any direct "porn" links from my site. Some pretty extreme politics and philosophical stuff, yes, but no dirty pictures. So I checked the page in question and tried the links from it, and found that one of them did indeed go to a porn site.

It turned out that what had happened was that the domain name of the site I had linked to was either sold by its former owner or allowed to expire at InterNIC due to nonpayment of renewal fees, and the domain was picked up by a new owner who's in the business of online pornography. This new owner set up the server so that links to any page on the old site would bring up the X-rated home page of the porn site, instead of just resulting in a "404 Not Found" error.

This illustrates a big risk for anyone who maintains links to other Web sites; places you link to can radically change their character, especially if domain names expire and get acquired by different parties. This may have a highly damaging effect on the reputation of a site that winds up with such a link, and the use of automated link-checking programs to weed out "404 Not Found" won't find this sort of problem.

--Dan

<http://www.softdisk.com/comp/dan/>

[This does remind us of the Intuit 800 number case "Risks of old documentation" that Richard C. Wolber contributed in [RISKS-](#)

[20.15.](#) PGN]

⚡ Virginia online sex offender database

Joe Thompson <joe@orion-com.com>

Tue, 19 Jan 1999 15:37:07 -0500

Virginia recently (December 29) released an online sex-offender database:

<http://sex-offender.vsp.state.va.us/Images/Search.htm>

In its first three weeks of operation, besides glitches involving names of offenders, two of 49 local residents whose addresses were published in a local weekly contacted them to say that the offender listed as living at that address has moved. The Virginia State Police have promised to update the database "swiftly".

Needless to say, the Virginia chapter of the ACLU is pointing to these errors as the exact reason they oppose the website. -- Joe

Joe Thompson Charlottesville, VA joe@orion-com.com

<http://kensey.home.mindspring.com/>

⚡ China solves the Millennium bug

Pete Mellor <pm@csr.city.ac.uk>

Sat, 16 Jan 1999 19:47:13 GMT

According to the BBC World Service yesterday, and various items in newspapers, China has solved its Millennium problems

(at least where air transport is concerned) at a stroke.

The chief executives of all of its airlines are ordered to be airborne at midnight on 31st December 1999.

Peter Mellor, Centre for Software Reliability, City University,
Northampton

Square, London EC1V 0HB, UK. Tel: +44 (171) 477-8422, Fax: +44
(171) 477-8585

[Apparently "only under consideration", not established. PGN]

⚡ Computer crash blew up radio listener's request messages

Kenji Rikitake <kenji@k2r.org>

Sun, 17 Jan 1999 13:54:57 +0900 (JST)

About 11:30pm EST, January 16, 1998, on CBC Radio One, Holger Petersen, the host of the program called Saturday Night Blues, said that he lost his listener's request voice messages due to "a computer crash" in CBC office in Edmonton, Alberta, Canada. Another proof of taking risk of NOT making backup data.

Kenji Rikitake <kenji.rikitaake@acm.org>, Toyonaka City, Osaka, JAPAN

⚡ REVIEW: "Stopping Spam", Alan Schwartz/Simson Garfinkel

"Rob Slade, doting grandpa of Ryan and Trevor" <rslade@sprint.ca>

Mon, 18 Jan 1999 11:44:23 -0800

BKSTPSPM.RVW 981030

"Stopping Spam", Alan Schwartz/Simson Garfinkel, 1998, 1-56592-388-X,
U\$19.95/C\$29.95
%A Alan Schwartz alansz@araw.mede.uic.edu
%A Simson Garfinkel simsong@vineyard.net
%C 103 Morris Street, Suite A, Sebastopol, CA 95472
%D 1998
%G 1-56592-388-X
%I O'Reilly & Associates, Inc.
%O U\$19.95/C\$29.95 800-998-9938 fax: 707-829-0104 nuts@ora.com
%P 208 p.
%T "Stopping Spam"

Eternal vigilance is the price of junk free email. Therefore, readers expecting to find a quick fix for spam in this book are possibly going to be disappointed. Those who persevere, however, will find much useful material that is both interesting, and valuable in the fight against unsolicited and commercial mass mail bombing.

Chapter one details the problem with a definition of spam, the functionally differing types of spam, the different intention of spam (including reputation attacks), and the reasons why spam should be combatted, rather than merely tolerated and deleted. A historical background to the situation is provided in chapter two. This includes mention of viral programs (plus a repetition of the myth that CHRISTMA EXEC caused a mass shutdown of VNET). the primary emphasis, though, is on the Green Card Lawyers, Cyberpromotions, and others of that ilk. (A warning against vigilante actions is also germane.) The current position is described very briefly in chapter three. Groups of spammers and spamming tools are noted. (Perhaps the authors do not

want to give anyone ideas, but the technology section is very terse indeed.) In closing, a nightmare future spam scenario is provided.

Chapter four provides a solid technical background for further discussion of spam, covering mail agents and the mail and news protocols. A number of steps that the average computer user can take are listed in chapter five. The range from hiding your identity or preventing address "harvesting" (not all the suggestions are convenient), to the more active detecting of spammers behind spoofing techniques, and reporting to authorities. Similar advice for newsgroups is given in chapter six, emphasizing specific programs like NoCeM.

Chapter seven moves into larger areas of responsibility with advice on both policy and practical configuration settings to reduce both incoming and outgoing spam. The larger net community is addressed in chapter eight.

An appendix lists a wide variety of resources, but the annotations may not always give you the complete picture. For example, the Spam Media Tracker Web site is listed, but at a relatively old address. This, of course, happens all the time on the net, but it is stranger that there is no mention of the spam-news mailing list, the original (and ongoing) source for the site.

It would, of course, be prohibitive to identify all international agencies dealing with spam. However, do note that only US government offices are noted as departments to report to.

While understandable, the tone of moral outrage that colours the

initial chapters may not be as helpful as a calmer precis. As the book hits its stride, though, it provides a good deal of helpful and useful information. All ISPs (Internet Service Providers), corporate network administrators, and net help desks should have a copy of this reference handy. Any serious Internet user will also find it well worth the price. As the authors put it, in slightly different words, the only thing necessary for the triumph of spammers is that good users do nothing.

copyright Robert M. Slade, 1998 BKSTPSPM.RVW 981030
rslade@vcn.bc.ca rslade@sprint.ca robertslade@usa.net
pl@canada.com

Find virus, book info <http://victoria.tc.ca/int-grps/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 20: Issue 18

Friday 29 January 1999

Contents

- ["When Doctors Make Mistakes"](#)
[Matt Blaze](#)
- [Celler beware? Cell-phone blockade](#)
[Sheri Alpert](#)
- [Distributed.Net & EFF Put Final Nail in DES Coffin](#)
[John Gilmore](#)
- [Trojan horse planted in TCP wrapper](#)
[PGN](#)
- [Internet vandals strike USIA Web site](#)
[Edupage](#)
- [Digital photos from drivers' licenses](#)
[Dan Gould](#)
- [Linux users want their money back from Microsoft](#)
[Edupage](#)
- [Y2K update turns city into deadbeat](#)
[Debora Weber-Wulff](#)
- [Programming errors](#)
[Fred Gilham](#)
- [Re: ... French announcement on crypto policy](#)
[Olivier MJ Crepin-Leblond](#)

- [Re: "Page-layout program hazards" and "Over-reliance on technology"](#)
[Don Byrd](#)
 - [Hotmail Web e-mail risk](#)
[Daniel P. Stasinski via others](#)
 - [Major security breach in Canadian consumer-tracking database](#)
[Wei-Yuen Tan](#)
 - [USENIX Security Symposium Call; Papers due March 9](#)
[Jennifer Radtke](#)
 - [REVIEW: "Bad Software", Cem Kaner/David Pels](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ "When Doctors Make Mistakes"

Matt Blaze <mab@research.att.com>

Mon, 25 Jan 1999 20:56:17 -0500

This week's New Yorker (dated February 1) has an excellent article, "When Doctors Make Mistakes," by Atul Gawande. The article, written by a surgical resident who was also a Clinton health policy advisor, offers a very nice summary of human error - and process failure - in various medical disciplines. The descriptions of widely varying user interfaces on different models of defibrilators or of design variations in anesthesia machine controls such that a clockwise turn of a knob increases dosage on some models and decreases on others should be familiar territory for RISKS junkies.

In a previous life, I worked briefly as a paramedic in New York, and I have actually performed many of the RISKy life-vs-death procedures, such as E-T intubation and tracheostomy, described in the first part of the

article. I recall never worrying much about killing someone by mistake - the training, culture, and protocols really were pretty well designed to make at least the most avoidable kinds of deadly errors reasonably unlikely (for example, we used only a limited number of models of defibrillator, and everyone everyone practiced frequently with all of them). What kept me up at night were worries of screwing up some non-life threatening procedure with grave consequences, like contributing to paralyzing an accident victim by rough handling, or failing to notice secondary injuries during an examination. These things were practiced and trained for rather less intensely than the more dramatic "life or death" procedures were.

Cryptography and computer security seems so much safer by comparison...

-matt

⚡ Celler beware? Cell-phone blockade

Sheri Alpert <salpert@gmu.edu>

Mon, 25 Jan 1999 11:50:57 -0500 (EST)

A GTE Wireless cellular tower in Crystal River, Florida, was rendered incommunicado whenever Calvin Simpson used his cell phone in his motor-home park, beginning on 4 Jan 1999. His phone was apparently tying up a control channel used to direct calls, and blocking all (other?) calls. After

tracking him down (it took 10 days), GTE gave him a different phone while

they tried to find out why it was causing the interference!

[Source:

Digital Flub: A Cell Phone's Knockout, *The Washington Post*, 25 Jan 1999,

F05, derived from an AP item; PGN Abstracting]

Sheri Alpert, PhD candidate, Institute of Public Policy
George Mason University, Fairfax, VA

⚡ Distributed.Net & EFF Put Final Nail in DES Coffin

John Gilmore <gnu@toad.com>

Thu, 28 Jan 1999 09:26:07 -0800

Tuesday, January 19, 1999

RSA Code-Breaking Contest Again Won by Distributed.Net and Electronic Frontier Foundation (EFF)

DES Challenge III Broken in Record 22 Hours

RSA DATA SECURITY CONFERENCE, SAN JOSE, CA -- Breaking the previous record

of 56 hours, Distributed.Net, a worldwide coalition of computer enthusiasts,

worked with the Electronic Frontier Foundation's (EFF) "DES Cracker," a

specially designed supercomputer, and a worldwide network of nearly 100,000

PCs on the Internet, to win RSA Data Security's DES Challenge III in a

record-breaking 22 hours and 15 minutes. The worldwide computing team

deciphered a secret message encrypted with the United States government's

Data Encryption Standard (DES) algorithm using commonly available technology. From the floor of the RSA Data Security Conference & Expo, a

major data security and cryptography conference being held in

San Jose,
Calif., EFF's DES Cracker and the Distributed.Net computers were
testing 245
billion keys per second when the key was found.

First adopted by the federal government in 1977, the 56-bit DES
algorithm
is still widely used by financial services and other industries
worldwide
to protect sensitive on-line applications, despite growing
concerns about
its vulnerability. RSA has been sponsoring a series of DES-
cracking
contests to highlight the need for encryption stronger than the
current
56-bit standard widely used to secure both U.S. and
international commerce.

"As today's demonstration shows, we are quickly reaching the
time when
anyone with a standard desktop PC can potentially pose a real
threat to
systems relying on such vulnerable security," said Jim Bidzos,
president of
RSA Data Security, Inc. "It has been widely known that 56-bit
keys, such as
those offered by the government's DES standard, offer only
marginal
protection against a committed adversary. We congratulate
Distributed.Net
and the EFF for their achievement in breaking DES in record-
breaking time."

As part of the contest, RSA awarded a \$10,000 prize to the
winners at a
special ceremony held during the RSA Conference. The goal of
this DES
Challenge contest was not only to recover the secret key used to
DES-encrypt
a plain-text message, but to do so faster than previous winners
in the
series. As before, a cash prize was awarded for the first
correct entry

received. The amount of the prize was based on how quickly the key was recovered.

"The diversity, volume and growth in participation that we have seen at Distributed.Net not only demonstrates the incredible power of distributed computing as a tool, but also underlines the fact that concern over cryptography controls is widespread," said David McNett, co-founder of Distributed.Net.

"EFF believes strongly in providing the public and industry with reliable and honest evaluations of the security offered by DES. We hope the result of today's DES Cracker demonstration delivers a wake-up call to those who still believe DES offers adequate security," said John Gilmore, EFF co-founder and project leader. "The government's current encryption policies favoring DES risk the security of the national and world infrastructure."

The Electronic Frontier Foundation began its investigation into DES cracking in 1997 to determine just how easily and cheaply a hardware-based DES Cracker (i.e., a code-breaking machine to crack the DES code) could be constructed.

Less than one year later and for well under U.S. \$250,000, the EFF, using its DES Cracker, entered and won the RSA DES Challenge II-2 competition in less than 3 days, proving that DES is not very secure and that such a machine is inexpensive to design and build.

"Our combined worldwide team searched more than 240 billion keys every second for nearly 23 hours before we found the right 56-bit key to decrypt the answer to the RSA Challenge, which was 'See you in Rome (second AES Conference, March 22-23, 1999),' " said Gilmore. The reason this message was chosen is that the Advanced Encryption Standard (AES) initiative proposes replacing DES using encryption keys of at least 128 bits.

RSA's original DES Challenge was launched in January 1997 with the aim of demonstrating that DES offers only marginal protection against a committed adversary. This was confirmed when a team led by Rocke Verser of Loveland, Colorado recovered the secret key in 96 days, winning DES Challenge I. Since that time, improved technology has made much faster exhaustive search efforts possible. In February 1998, Distributed.Net won RSA's DES Challenge II-1 with a 41-day effort, and in July, the Electronic Frontier Foundation (EFF) won RSA's DES Challenge II-2 when it cracked the DES message in 56 hours.

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>.

[Thanks to all of you who commented on my incomplete reportage. Deep Crack lucked out on only 9% of the key space, whereas Distributed

Crack as a whole cranked through 22.2% of the key space.

My hasty note from the RSA Conference in [RISKS-20.17](#) was based on a

desire to report the crack in the absence of the fuller story, which is

included above. It is clear that the DEEP CRACK exercise represents

a rude awakening for those remaining folks (such as those who had touted

export controls above 40-bit keys) who believed that such a machine could

not be built. But the deeper message of course is that we no longer even

need such a machine -- if vast portions of the total world-wide resources

of the Net were mobilized, it would be possible for WORLD CRACK to break

56-bit DES in a few seconds, plus whatever e-mail delay was needed to

report the crack by the lucky participant whose machine found the key!

Once again, a little realism is needed. PGN]

Trojan horse planted in TCP wrapper

"Peter G. Neumann" <Neumann@CSL.sri.com>

Fri, 22 Jan 1999 11:09:33 -0500

At least 52 computer systems downloaded a TCP wrapper program directly from a distribution site after the program had been contaminated with a Trojan horse early in the morning of 21 Jan 1999. The Trojan horse provided trapdoor access to each of the contaminated systems, and also sent e-mail identifying each system that had just been contaminated. The 52 primary sites were notified by the CERT at CMU after the problem had been detected and fixed. Secondary downloads may also have occurred. [Source: Elizabeth Corcoran, Hackers Strike Popular Program; 52 Computers Downloaded 'Trojan Horse' Allowing Outside Access, *The Washington Post*, 22 Jan 1999, page E03; PGN Abstracting]

⚡ Internet vandals strike USIA Web site

Edupage Editors <edupage@franklin.oit.unc.edu>

Thu, 21 Jan 1999 14:36:15 -0500

The Web site of the United States Information Agency, which is used by American diplomats abroad for statements on American policy or texts of official speeches, was broken into recently by Internet vandals who left on the USIA system a "Trojan Horse" piece of computer code that caused basic hardware damage and the destruction of the site. A USIA computer specialist

said security for the site will be beefed up. "We simply can't have this happening every six months. People rely on us." (*The New York Times*, 21 Jan 1999; Edupage 21 Jan 1999)

⚡ Digital photos from drivers' licenses

Dan Gould <dlg@cs.brown.edu>
Fri, 22 Jan 1999 05:58:10 -0500 (EST)

For the first time since authorities began snapping photographs of drivers for licenses, state officials have begun selling the images wholesale. ... South Carolina has released 3.5 million digital photographs, Florida has started the process of transferring 14 million images in its files and other states have expressed interest in doing the same. ... While it has long been customary or a legal requirement to restrict access to driver photos to law enforcement authorities, company officials pledged to handle their new storehouse of digital pictures carefully. [Excerpted from an article by Robert O'Harrow Jr., *The Washington Post*, A01, 22 Jan 1999]

⚡ Linux users want their money back from Microsoft

Edupage Editors <edupage@franklin.oit.unc.edu>
Tue, 26 Jan 1999 14:08:04 -0500

Aficionados of the Linux operating system, which is available for free, say

they will demand their money back for Windows software installed against their wishes on PCs they buy. Their demand is based on a Windows licensing agreement that says that if the purchaser does not agree to the terms and conditions of use of the Windows software, he or she should promptly contact manufacturer for instructions on return of the unused product for a refund. Microsoft says that agreement applies only to the issues surrounding the of making copies of the software. (*The New York Times*, 25 Jan 1999; Edupage, 26 January 1999)

[Various marches on Microsoft offices are apparently being planned. PGN]

⚡ Y2K update turns city into deadbeat

Debora Weber-Wulff <Debora.Weber_Wulff@te.mah.se>
Wed, 27 Jan 1999 10:02:17 +0100

Sydsvenskan, 19. Jan 1999 [paraphrased by dww]

The city of Malmo[e] in the south of Sweden updated its bookkeeping software in October in order to get ready for the year 2000. The program AdeEko by Enator takes care of paying the bills for the city.

But since it has been updated, some bills are not being paid. When the clerks leave their offices in the evening, everything looks great. But sometime during the night, the system knocks itself out, and forgets to send the rest of the files with the payments to the banks and the post office.

This has happened every night since the system has been installed, and no one knows why. Enator is having people babysit the system over night in attempts to find out what is wrong. It takes a very long time for the bills to be paid, as the clerks must sort through which ones were paid and which ones weren't. The babysitters watch for bills which knock out the system, remove them, and restart the system.

A spokesperson for Enator identified the problem as being simply files that should be going to the banks and the post office not being accepted there, but he is not accusing anyone of anything. The search continues...

Debora Weber-Wulff MALMOe HOeGSKOLA 205 06 Malmo SWEDEN
Tel: +46-40-6657354 (Fax: -031) Debora.Weber_Wulff@te.mah.se

Programming errors

Fred Gilham <gilham@csl.sri.com>
Thu, 28 Jan 1999 18:35:19 -0800

I am reminded again of how shaky the software world is.

Someone has been making a major effort to clean up the code in the FreeBSD tree. In two days he has reported three instances of the following common C error:

```
if (x = y)
```

instead of

```
if (x == y)
```

This is in running code, in an OS whose developers consider stability to be one of its major advantages over other offerings.

He also reported some missing breaks in a switch statement---many of us remember what THAT error did not too long ago. [[RISKS-9.61](#) to [71](#).

Trojan horse switches in midstream? PGN]

-Fred Gilham gilham@csl.sri.com

🚩 Re: ... French announcement on crypto policy ([RISKS-20.17](#))

"Olivier MJ Crepin-Leblond" <ocl@gih.com>

Thu, 21 Jan 1999 12:56:13 -0000

This, while being a total reversal of policy from the laws of 1996, is in fact the right way forward, and makes sense. I would expect other governments to adopt the same policy soon.

The previous law was seriously curbing the French industry's use of cryptography for its transfers of sensitive information, thus putting them at a disadvantage when it comes to industrial espionage. Because, let's face it, with the fall of the Iron Curtain, 99.9% of the world's espionage is now industrial espionage. Globalization has made stakes in international trade so important that corporations need to know what their competitors do, and the press has been very verbose about past scandals that have come into the

open.

I suspect that the assumption made by the French government are:

1. ultimately, no code is unbreakable;
2. the legal authorities will have the power to prosecute if an entity refuses to provide them with the key to suspicious encoded data.

What about personal privacy ?

Privacy is a myth, which you and I believe in; aren't we naive ?

Olivier MJ Crepin-Leblond, Ph.D. - ocl@gih.com
Global Information Highway Limited

✉ Re: "Page-layout program hazards" and "Over-reliance on technology"

Don Byrd <dbyrd@cs.umass.edu>
Tue, 26 Jan 1999 16:19:26 -0500

I've been trying to avoid responding to this discussion, but I can't ignore it any longer.

As a user-interface researcher and designer, I've seen way too many solutions to the problems bad UIs cause along the lines of "understand your tools", "read the manual carefully", etc. TROFF's UI is a bad one. (This should be no surprise, since most UNIX programs, especially old ones, have bad UIs :-) ; it was a reasonable UI for when it was designed.) Training people to handle a poor UI better is very difficult, and even if

Resent-From: 0xdeadbeef@substance.blackdown.org

Forwarded-by: Nev Dull <nev@bostic.com>

[Background: Someone hacked the win.tue.nl ftp site and installed versions of various packages that would forward user login/uid information to Hotmail addresses.]

=====

From: "Daniel P. Stasinski" <dannys@KAREMOR.COM>
Subject: Microsoft Hotmail

I contacted Microsoft/Hotmail asking them to close the account that was listed in the backdoored tcp wrapper source code. I also forwarded the offending code.

The word back from them is that they will not close it. Theft of passwords and hacking does not violate their terms of service.

Daniel P. Stasinski, Software Engineer, Karemor International, Inc.
2406 South 24th Street, Phoenix, AZ 85034 dannys@karemor.com

🚨 Major security breach in Canadian consumer-tracking database

Wei-Yuen Tan <monkeyboy@pobox.com>
Fri, 22 Jan 1999 20:32:15 -0500

Excerpted from the Toronto **Globe and Mail** (Canada) on 22 Jan 1998

Supposedly confidential records of up to 50,000 Canadians were accidentally left accessible to the general public on the Website of Air Miles, Canada's

second largest customer loyalty program. Fortunately, the records exposed on the Website, www.airmiles.ca, were only those of potential customers who had filled out an online application form. However, very sensitive information pertaining to these 50,000 individuals was openly accessible online until the Website was taken offline mid-morning Thursday 21st Jan. The Website will remain offline until its operators are able to resolve the issue.

Air Miles tracks the consumer behavior of its five million Canadian cardholders (almost 20% of our population), tracking such information as:

- purchasing history
- name, address, telephone numbers and e-mail addresses.
- credit ratings, credit cards held, bank records
- vehicle and property ownership
- for business subscribers, company name, address, industry and ranges for annual revenue, number of employees and number of locations.

Air Miles, as the name implies, attracts customers by offering airline reward miles for purchases made at participating retailers.

Despite my consistent efforts to discourage them, my parents have been faithful cardholders for several years. Apparently they have finally accumulated

enough points for a trip to our neighbour's house across the street.

A RealVideo news clip of the subject is available from the CBC Website at the following URL:

<http://www.newsworld.cbc.ca/cgi-bin/templates/view.cgi?/news/1999/01/22/airmiles990122>

Wei-Yuen Tan <monkeyboy@pobox.com>

✦ USENIX Security Symposium Call; Papers due March 9

Jennifer Radtke <jennifer@usenix.ORG>

Fri, 22 Jan 1999 17:57:32 GMT

8th USENIX Security Symposium

August 23-26, 1999

Washington, D.C., USA

Sponsored by USENIX in cooperation with The CERT Coordination Center

If you are working in any practical aspects of security or applications of cryptography, the program committee urges you to submit a paper.

Dates for Refereed Paper Submissions: March 9, 1999.

The full Call for Papers is at <http://www.usenix.org/events/sec99/> .

The Symposium brings together researchers, practitioners, system administrators, system programmers, and others interested in the latest advances in security and applications of cryptography. Two days of tutorials will be followed by two days of technical sessions, offering refereed papers, invited talks, works-in-progress, panel discussions, and a product exhibition.

Invited Talk Speakers include:

Ross Anderson, Computer Laboratory, Cambridge University

Ed Felten, Princeton University

Susan Landau, University of Massachusetts

Peter G. Neumann, SRI

Paul Van Oorschot, Entrust Technologies

Marcus Ranum, Network Flight Recorder

USENIX is the Advanced Computing Systems Association. Our international membership includes engineers, system administrators, scientists, and technicians. Our conferences are recognized for delivering pragmatic, technically excellent information in a highly interactive, vendor-neutral forum.

🔥 REVIEW: "Bad Software", Cem Kaner/David Pels

"Rob Slade" <rslade@sprint.ca>
Wed, 27 Jan 1999 08:35:17 -0800

BKBDSFWR.RVW 981122

"Bad Software", Cem Kaner/David Pels, 1998, 0-471-31826-4,
U\$29.99/C\$42.50

%A Cem Kaner

%A David Pels

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 1998

%G 0-471-31826-4

%I John Wiley & Sons, Inc.

%O U\$29.99/C\$42.50 416-236-4433 fax: 416-236-4448

%P 365 p.

%T "Bad Software: What to Do When Software Fails"

Bad software. Isn't that phrase redundant?

This book is **not** about viruses, trojans or other malware. It talks about software that doesn't work as it should, and what you can, or should, do about it.

Chapter one is a kind of beginner's panic guide to getting a refund. It's

quite practical, although those used to fighting their way through the retail bureaucracy will find little new. On the other hand, most people aren't used to that particular battle, so the book will have a fairly wide audience. One proviso: when it gets to legal issues, as with all too many such books, the material is strictly US-centric. Chapter two is not very clear, up front, as to what it is for. Ultimately it says a lot about the problems at software publishing houses, and not very much about yours. While this might make you more (or less) understanding of the problem, the advice given in chapter three is much more useful. It does tend to be of the same variety as that given in the troubleshooting sections of most documentation, but the second section, dealing with reasonable expectations of software and representations, is quite good. Judging by the number of pages, chapter four starts to get into the comfort zone of the authors: figuring out a negotiating position. This is a good template to follow, setting out all aspects of the problem and its significance, and providing good standards for what is reasonable to expect and what is not. Chapter five covers the support or complaint call itself, and, again, is reasonable, but nothing new.

Chapter six reviews the various types of consumer protection agencies. Again, when dealing with the governmental departments, the material only applies to the US (and this holds for chapters seven through ten as well). However, the coverage is both reasonable and practical, noting,

for example,
that the loudly vaunted Better Business Bureau is funded by
business, not by
consumers, and is a franchise operation that varies in operation
from place
to place. Warranties, disclaimers, and misrepresentation are
discussed in
chapter seven, with illustrations both from statutes and
numerous cases. An
outline of the process for a lawsuit is provided in chapter
eight. Chapter
nine looks at negotiating with lawyers. The procedure and
limitations for
small claims court are given in chapter ten. The final chapter
gives some
general advice on shopping, and being a careful consumer.

This work does give you advice, breathing space, and a roadmap
for pursuing
a complaint about software. It is appropriate for neophytes in
computer
use: not only the home hobbyist, but the beginning technical
support person
in a larger office. However, as my wife pointed out when I was
describing
the book, the biggest issue for most such people is having the
confidence to
know that the software, and not you, are at fault, and there the
text is of
less use. The strengths of the book are in negotiating tactics,
and in a
dispassionate view of what you might be able to expect.
Although, if you
have the experience to know what is reasonable you won't need
the book, and
if you have little enough experience that you need the book you
probably
don't know enough to be comfortable standing up to some snooty
techie.

copyright Robert M. Slade, 1998 BKBSDFWR.RVW 981122
rslade@vcn.bc.ca rslade@sprint.ca robertslade@usa.net
pl@canada.com

[Is the phrase "Bad software" *redundant*? If people learn how to write bad software in school, it must be a *taught-ology*! 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 20: Issue 19

Monday 1 February 1999

Contents

- [Complete ATC power failure in the U.S. Northwest](#)
[Paul Cox](#)
- [NYC 911 crash](#)
[David Lesher](#)
- [New attack on PGP keys with a Word Macro](#)
[Fred Cohen](#)
- [Intel's Pentium III Processor ID](#)
[Bruce Schneier](#)
- [Risks of successful security software](#)
[Nick Brown](#)
- [About the most bizarre Microsoft message yet](#)
[Fred Cohen](#)
- [Risks of using Windows95 as an embedded system](#)
[Steven J. Greenwald](#)
- [Government computer withholds benefit from British widows](#)
[Pete Mellor](#)
- [Re: not a Hotmail Web e-mail risk](#)
[John R Levine](#)
- [REVIEW: "The Transparent Society", David Brin](#)
[Rob Slade](#)

- [CFP: New Security Paradigms Workshop 1999](#)
[Mary Ellen Zurko](#)
 - [SEPG '99: 11th Software Engineering Process Group Conference](#)
[Carol Biesecker](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈ Complete ATC power failure in the U.S. Northwest

"Paul Cox" <pcox@eskimo.com>
Sun, 31 Jan 1999 22:36:22 -0800

Some time back, I wrote about some of the various risks involved with air-traffic control computer-communication systems. I mentioned how even with backup systems controllers are still extremely vulnerable to the power going out.

Well, it happened. On 15 Jan 1999, at 2 pm, the power failed at Seattle Center, an en-route ATC facility that covers nearly 300,000 square miles of the NW United States. I had the unusually good luck **not** to be at work at the time.

The power failed during a normal, routine quarterly test procedure on the power supply units. To be honest, I don't understand the technical side of how/why the power failed; I had it explained and I still didn't get it. But the gist of it was that during the test, a circuit board didn't do what it was supposed to, and there was a very brief (less than a second) interruption of the power to our systems.

Unfortunately, our systems cannot handle any interruption, and thus all the

computers had to be rebooted and recalibrated. Our communication systems failed completely, as they are totally computer-dependent, digitized, touch-screen interface modules. This system took over a half-hour to reload.

Our main radar displays all went out as well, and the backup display system failed too. It took anywhere from 45 to 75 minutes for any radar displays to come back at various sectors in the building.

Recall my description of how frantic controllers are when suddenly the separation requirements for aircraft go from 5 miles to 20 miles (radar environment to non-radar)? That is exactly what happened.

The only system that DID work is a hard-wired, emergency radio backup system that only needs power to be supplied to it, but which is old-fashioned enough that it doesn't have computers running it. Ironically, we had to fight and fight and fight to have this system installed when our recent upgrades took place.

Without it, we would have been completely helpless to communicate with any aircraft in the area. With it, we were able to restore limited ATC service within a couple of minutes, falling back on the "good old days" method of pilots staying on specific airways, reporting their progress over certain points on the ground, and using paper strips, pencils, and our heads to figure out whether anyone was in conflict with anyone else.

This failure simply drives home yet again that backup systems

are only as good as the main systems IF those backups are equally dependent upon a power supply. In fact, our backup communications system and backup radar display systems were essentially worthless to us, because they failed at the same instant as the main system did when the power died.

As long as you have a single point of failure in any system, it doesn't matter how many backups you have downstream if they are dependent on that point.

Fortunately, we still had the old-fashioned radios, not to mention the Mark I Human Brain Wet Computers working for us.

Paul Cox ZSE

NYC 911 crash

David Leshner <wb8foz@nrk.com>
Mon, 1 Feb 1999 11:33:58 -0500 (EST)

<<http://www.newsday.com/ap/rnmpmt08.htm>> and wire reports.

NYC 911 went down during a backup generator test. The backup system did not function.

It took an hour to get the fallback running, and six hours to restart the main system. There were 4-per-year tests of the generators; but one wonders how frequently the fallback system was deployed.

The RISK? Testing for failures often succeeds, but not where you

thought.

In the "still works" department, a local reports NYC still has fireboxes, and they were up. This is one of those "too simple to improve" technologies -- a DC loop with clockwork-driven mechanical pulsers shorting to ground. Break the loop and the boxes STILL work on the remaining leg.

voice (301) 56-LINUX

[An AP item contributed by "corinsee" noted that a Vermont man died of an apparent heart attack during the outage while waiting for 911 to answer. Many other RISKS readers commented on this case as well. PGN]

🔥 New attack on PGP keys with a Word Macro

Fred Cohen <fc@all.net>

Fri, 29 Jan 1999 23:11:40 -0800 (PST)

I just got a look at a Word file (CALIG.DOC) that contains user IDs and passwords to pornographic sites. In addition to these pointers, it has a Trojan Horse that finds the user's private PGP key ring and ftp's it to:

```
209.201.88.110 (codebreakers.org)
user anonymous
password itsme@
directory incoming
binary mode
stored name: NewSecRingFile[0-9][0-9][0-9][0-9]
```

This Trojan does its job in visual basic and - except for the initial notice

(if enabled) that macros are present - gives no indication of this function that it performs. I figure the best defense against this is to:

- 1) Have thousands of users ftp phony files to that IP address and filename on a regular basis, thus making it impossible to get any real PGP keys - preferably send valid-looking PGP keys so they have to waste a lot of time cracking them.
- 2) Cut off all service for ftp with 209.201.88.110 (codebreakers.org)
 - either at the ISP, at your gateway, or at the borders to your country.
- 3) Prosecute for possession of access devices - with international cooperation between authorities.
- 4) Tell your people that this has been done so they will stop looking at pornography listing files (fat chance this will work).

At any rate, I hope that you will take prudent precautions within your organization against this potential attack on the security of your private keys.

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

[Much-too-long disclaimer omitted, separating the two roles. PGN]

Intel's Pentium III Processor ID

Bruce Schneier <schneier@counterpane.com>

Mon, 01 Feb 1999 17:05:03 -0600

Now is probably a good time to summarize the controversy regarding Intel's Processor ID.

At the RSA Conference last month, Intel announced that it would be embedding a unique ID number into every processor it sold:
<http://www.redherring.com/insider/1999/0120/news-inteldongle.html>
<http://www.zdnet.com/zdnn/stories/news/0,4586,2190019,00.html>

My initial comments, posted to ZDNet News, were as follows
<<http://www.zdnet.com/zdnn/stories/comment/0,5859,2194863,00.html>>:

Why Intel's ID tracker won't work
By Bruce Schneier, ZDNet News
January 26, 1999 4:45 PM PT

Last Thursday Intel Corp. announced that its new processor chips would come equipped with ID numbers, a unique serial number burned into the chip during manufacture. Intel said that this ID number will help facilitate e-commerce, prevent fraud and promote digital content protection. Unfortunately, it doesn't do any of these things.

To see the problem, consider this analogy: Imagine that every person was issued a unique identification number on a national ID card. A person would have to show this card in order to engage in commerce, get medical care, whatever. Such a system works, provided that the merchant, doctor, or whoever can examine the card and verify that it hasn't been forged. Now imagine that the merchants were not allowed to examine the card. They had

to ask the person for his ID number, and then accept whatever number the person responded with. This system is only secure if you trust what the person says.

The same problem exists with the Intel scheme.

Too easy to hack

Yes, the processor number is unique and cannot be changed, but the software that queries the processor is not trusted. If a remote Web site queries a processor ID, it has no way of knowing whether the number it gets back is a real ID or a forged ID. Likewise, if a piece of software queries its processor's ID, it has no way of knowing whether the number it gets back is the real ID or whether a patch in the operating system trapped the call and responded with a fake ID. Because Intel didn't bother creating a secure way to query the ID, it will be easy to break the security.

As a cryptographer, I cannot design a secure system to validate identification, enforce copy protection, or secure e-commerce using a processor ID. It doesn't help. It's just too easy to hack.

This kind of system puts us in the same position we were in when the government announced the Clipper chip: Those who are engaged in illicit activities will subvert the system, while those who don't know any better will find their privacy violated. I predict that patches that randomize the ID number will be available on hacker Web sites within days of the new chips hitting the streets.

The real question

The only positive usage for processor IDs is the one usage that Intel said they would not do: Stolen processor tracking. Pentium II chips are so valuable that trucks are hijacked on the highways, sometimes resulting in drivers being killed. A database of stolen processor IDs would drop the market for stolen CPUs to zero: Board manufacturers, computer companies, resellers and customers could simply query the database to ensure that their particular CPU wasn't stolen. (This is the primary usage for automobile VINs.) This same system could be used to prevent manufacturers from overclocking their CPUs -- running them faster than Intel rated them for -- another thing that Intel would love to prevent.

The real question is whether computers are a dangerous technology, and need to be individually tracked like handguns and automobiles. During the Cold War many Eastern European countries required mimeograph machines to be individually licensed; I have a hard time believing that computers need the same sorts of controls.

The controversy has been furious. EPIC announced an Intel boycott (See <http://www.bigbrotherinside.com/> for a good summary of the issues).

Intel backed off, saying that the feature would be initially turned off, (see <http://www.zdnet.com/zdnn/stories/news/0,4586,2192717,00.html>), then

admitted that they had always intended to throw this bone to privacy groups.

More interesting were reports that there would be some kind of access

protocol designed to randomize the ID for different websites:

<http://www.eet.com/story/OEG19990127S0011>

http://www.eetimes.com/printableArticle?doc_id=OEG19990127S0033

And others have pointed out that dedicated hardware IDs have been around

for a while: Ethernet cards, hard drive IDS, etc.

So what's the difference, and what's the point? Intel is pushing this

scheme as a way to prevent fraud. I argued above, and I still maintain,

that it fails in that regard. Even with the addition of a software

protocol, there is no way to prevent a program from intercepting the call

and replacing the ID number with a phony one. I don't like this scheme not

because there's a unique ID, but because Intel is making impossible promises

about its utility.

Free crypto newsletter. See: [http://www.](http://www.counterpane.com)

[counterpane.com](http://www.counterpane.com)

Bruce Schneier, President, Counterpane Systems Phone: 612-823-1098

101 E Minnehaha Parkway, Minneapolis, MN 55419 Fax: 612-823-1590

✶ Risks of successful security software

BROWN Nick <Nick.BROWN@coe.fr>

Mon, 1 Feb 1999 09:24:57 +0100

The Daily Telegraph (London) reports that a hacker was so outraged when he failed to beat the challenge laid down by Paul Smith, creator of network security software called Access Denied, that he hacked into Mr. Smith's credit records instead. Mr. Smith is now trying to clear up a string of false court judgements against him so that he can apply for a home loan.

Apparently the hacker was avenging his failure to break Access Denied, having previously boasted to friends that he could do it in five minutes.

This would appear to indicate what might perhaps be considered an age-old

RISK: if you implement security measures professionally, make sure you can't be identified personally by those potentially excluded by your measures.

Difficult to follow completely when your aim is to sell your software...

Nick Brown, Strasbourg, France

✦ About the most bizarre Microsoft message yet

Fred Cohen <fc@all.net>

Sun, 31 Jan 1999 07:35:42 -0800 (PST)

I just got perhaps the most bizarre Microsoft error of all time. I was copying files from a network drive to a Jazz drive, and up pops an error box with the message "Cannot copy sensitive countries" - at which point the copy of all the files failed! It stopped on a filename corresponding to a country

whose name may well be on the sensitive countries list.

I guess Microsoft doesn't want us to use the names of certain countries in our files!

Fred Cohen of
Fred Cohen & Associates: <http://all.net> - fc@all.net - tel/
fax: 925-454-0171

⚡ Risks of using Windows95 as an embedded system

"Steven J. Greenwald" <sjg6@gate.net>

Sat, 30 Jan 1999 21:07:38 -0500

This is really a case of a picture being worth ten thousand words, as the Chinese old proverb says. I urge readers to take a look at <<http://home.studit.com/com00120/sparbanken1.jpg>> and see what is possibly the most foolish bank in the world.

If you can't view the picture, it shows a bank ATM, with the screen showing a Windows95 error message. I can't tell what it says, as I am not fluent in Swedish.

The risks here are so obvious it defies rationality as to why this bank decided to do this.

Steven J. Greenwald <http://www.gate.net/~sjg6>

⚡ Government computer withholds benefit from British widows

Pete Mellor <pm@csr.city.ac.uk>

Sat, 30 Jan 1999 17:30:28 GMT

From the "Moneybox" programme on BBC Radio 4 this morning:-

A computer system installed at a total cost of 140 million pounds sterling (said to be the largest civilian system in Europe) is responsible for underpayment of widows' benefits in the UK.

The system was originally scheduled for completion in February 1997. The contractors now expect the remaining subsystems to be installed in March of this year. Problems have apparently been caused by "software bugs", although it was not clear from the programme to what extent software faults, as opposed to late and incomplete delivery, are responsible for the trouble.

The basic problem appears to be that it has not been possible to input complete and up-to-date records of all National Insurance contributions, on which the widow's benefit is calculated.

The effect has been that women entitled to widow's benefit have been underpaid for a period of up to two years by amounts ranging from one pound to 100 pounds per week. The UK government in the meantime is sitting on one billion pounds in unpaid benefits, and the interest that is accruing on this.

There are a lot of angry widows beating on the doors of the Department of Social Security. So far, they have not received an awful lot of help. A short time ago, the Liberal Democrat MP David Rendell drew attention to the scandal by a question in Parliament. Steven Timms, Minister of

State for
Social Security, said in interview on the programme that, from
the 6th
January of this year, all *new* claimants would be paid
correctly. He stated
that the NI contribution records would be up-to-date by the end
of March,
and that existing beneficiaries whose total underpayment
exceeded 100
pounds, and whose payment due for lost interest exceeded 10
pounds, would
automatically be reimbursed by lump sum payments for both
underpaid benefits
and interest.

The government has set up a task force to deal with enquiries:-

NI Benefit Task Force, Benefits Agency Department ST, Quarry
House,
Quarry Hill, Leeds LS2 7AU

I have quoted the above from memory, reinforced by a 'phone call
to Radio 4
enquiries. Although I have tried to be as accurate as possible,
anyone who
requires further details should send a SAE to:-

Fact Sheet Week 5, Moneybox, Room 6239, BBC Television Centre,
Wood Lane, Shepherds Bush, London W12 7RJ

Apparently, reports from current affairs programmes such as
Moneybox are not
held on the BBC's website, due to lack of staff to input them.
However, a
detailed report also appeared in The Times on 26th January.

Peter Mellor, Centre for Software Reliability, City University,
London
EC1V 0HB, UK. Tel: +44 (171) 477-8422 p.mellor@csr.city.ac.uk

⚡ Re: not a Hotmail Web e-mail risk (Stasinski*, [RISKS-20.18](#))

John R Levine <johnl@iecc.com>

Sun, 31 Jan 1999 17:44:00 -0500 (EST)

This sounded pretty unlikely to me, so I asked the head of Hotmail's abuse department about it. He says that the drop box was cancelled promptly, and they notified Mr. Stasinski.

John Levine, johnl@iecc.com, Primary Perpetrator of "The Internet for Dummies", Information Superhighwayman wanna-be, <http://iecc.com/johnl>, Sewer Commissioner

⚡ REVIEW: "The Transparent Society", David Brin

"Rob Slade" <rslade@sprint.ca>

Fri, 6 Nov 1998 11:19:57 -0800

BKTRASOC.RVW 980919

"The Transparent Society", David Brin, 1998, 0-201-32802-X, U \$25.00/C\$34.95

%A David Brin

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario M3C 2T8

%D 1998

%G 0-201-32802-X

%I Addison-Wesley Publishing Co.

%O U\$25.00/C\$34.95 416-447-5101 fax: 416-443-0948 bkexpress@aw.com

%P 378 p.

%T "The Transparent Society"

As the author points out, this book will probably be shelved alongside texts on privacy. It is, however, more properly about candour. I

find,
therefore, that I must make an admission of a rather important bias.
Despite being considered by some to be a security expert, I have never had any particular interest in the practice of privacy and confidentiality. I am much more interested in openness.

Part one looks at the new transparent world as access to all kinds of information increases. Chapter one points out that the time to discuss whether we want technology or privacy has passed: technology is here, and it *will* provide access to information, and erode privacy, whether we like it or not. Brin does suggest that we still have a choice about the management of that technology. Do we want to have all data available only to a select few (such as the government), or all data available to everyone? The "information age" is reviewed in chapter two, but there is also a very interesting examination of the possibility of the resurgence of amateur scholarship. Various current invasions of, and attacks on, privacy are discussed in chapter three. In response to these, and in opposition to the usual calls for more legislated protections on privacy, Brin proposes reciprocal transparency: everyone who wants to collect information on the public must make the same information about themselves publicly available. Chapter four raises an extremely interesting point in relation to copyright, patent, and other legal restrictions on intellectual property, and the fact that the information age seems to have so much trouble with it. Transparency initially seems to threaten to totally destroy the

idea of
copyright, but ultimately may present a unique solution to
maintaining its
proper function.

Part two looks at those problems involved in an open society.
Chapter five
presents some of the arguments that should be reviewed, from the
toxicity of
ideas to the irony of western civilization's delight in
individualism. The
inherent benefits of accountability are reiterated in chapter
six, although
with less eloquence and insight than earlier text displayed.
The encryption
debate is a convoluted one, and is fairly, but rather unclearly,
portrayed
in chapter seven. The general tone of most of the book is
libertarian, so
the author does not seem to be completely comfortable with
arguing against
the merits of confidentiality of communications. It is,
however, ironic
that Brin does not report the later research of Dorothy Denning
that
indicates law enforcement agencies really do not need the
ability to break
encryption, since in an odd way it strengthens his central
thesis.

Part three proposes some means of achieving an open society.
Chapter eight
reviews a number of tools for transparency, but manages to look
ragged and
disorganized. Some future technological "tools races" are
described with a
bit more coherence in chapter nine. The various arguments in
favour of
openness are extended, in chapter ten, to the international
arena. Chapter
eleven closes off with a summation of the rest of the book.

Since Brin is well known as a popularizer of science and as a

science
fiction writer, and since his scientific training is not in the
field of
information technology it would be easy to see this book as yet
another
attempt by someone to trade on a reputation and a currently
popular field in
order to make a few bucks with minimal effort and thought.
Although his
writing background has helped to produce a text that is easily
readable, the
work is informed by a thorough understanding of the issues and
technologies,
and also leavened with insight and wit. Unfortunately, most of
the really
good stuff comes in the first four chapters, leaving the rest of
the volume
somewhat anticlimactic.

The book is both reasonable and provocative, and makes an
interesting
counterpoint to much of the current discussion of privacy and
technology.
Discussions of the important topics of privacy and encryption
are both
balanced and quite complete, providing those near to the fields
with a
useful primer. In addition, Brin's more controversial points
are well
taken, and deserve serious consideration.

copyright Robert M. Slade, 1998 BKTRASOC.RVW 980919

✶ CFP: New Security Paradigms Workshop 1999

<Mary_Ellen_Zurko@iris.com>
Mon, 1 Feb 1999 09:17:57 -0500

Call For Papers
New Security Paradigms Workshop 1999

A workshop sponsored by ACM
22 - 24 September 1999
Caledon Hills, Ontario, Canada
<http://www.nspw.org>

[Starkly abridged for RISKS. PGN]

The 1999 New Security Paradigms Workshop will take place from September 22 - 24, 1999 at The Millcroft Inn, an hour north of Toronto, Ontario, Canada.

In order to preserve the small, intimate nature of the workshop, participation is limited to authors of accepted papers and conference organizers. Because these are new paradigms, we cannot predict what subjects will be covered. Any paper that presents a significant shift in thinking about difficult security issues will be welcomed.

Program Co-Chairs:

Steven J. Greenwald
2521 NE 135th Street
North Miami, FL 33181 USA
e-mail: sjg6@gate.net
voice: (305) 944-7842
fax: (305) 944-5746

Cristina Serban
AT&T Labs
307 Middletown-Lincroft Rd.
Lincroft, NJ 07738 USA
e-mail: cserban@att.com
voice: (732) 576-3279
fax: (732) 576-6406

[See <http://www.nspw.org> for the full call for papers.
The deadline for electronic submissions is 2 Apr 1999 --
alternatively, 26 Mar 1999 for hardcopy. PGN]

SEPG '99: 11th Software Engineering Process Group Conference

Carol Biesecker <cb@SEI.CMU.EDU>
31 Jan 1999 20:01:46 GMT

SEPG '99 - The 11th Software Engineering Process Group (SEPG) Conference

Software Process Improvement (SPI) Investments Today for a Changing Tomorrow

March 8-11, 1999, Hyatt Regency Atlanta, Atlanta, Georgia

FEB. 3, 1999 - Deadline for Early Bird Registration Discount

For complete details, including the preliminary program and information

visit the SEI Web site at

<http://www.sei.cmu.edu/products/events/sepg/>

Download the registration form, available in portable document format

(PDF), then print, complete, and return this form to:

Events, Software Engineering Institute

Carnegie Mellon University

Pittsburgh, PA 15213-3890

FAX: 412 / 268-7401

The complete Preliminary Program is also available at the same Web site

in portable document format (PDF) for downloading or printing.

The



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 20

Weds 10 February 1999

Contents

- [Spanish bank buy lots of shares because of Euro problems](#)
[David Mediavilla](#)
- [E-Trade computers crash again -- and again](#)
[Edupage](#)
- [Copier quota exceeded](#)
[Philip Koopman](#)
- [Risks of Furbies: NSA was right!](#)
[Pete Mellor](#)
- [State of the states in Y2K readiness](#)
[Edupage](#)
- [The NT Blue Screen of Death](#)
[Bruce Wampler](#)
- [The risks of "standard" software?](#)
[Rob Slade](#)
- [You are still in France](#)
[Adam Shostack](#)
- [It gets weirder every day...](#)
[Fred Cohen](#)
- [The risks of shopping at Amazon](#)
[Ross Anderson](#)

- [Re: Risks of successful security software](#)
[Pete Mellor](#)
 - [Re: Government computer withholds benefits ...](#)
[Pete Mellor](#)
 - [FMICS4 call for papers](#)
[Diego Latella](#)
 - [REVIEW: "Mercury Rising", Douglas Pearson Ryne](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Spanish bank buy lots of shares because of Euro problems

David Mediavilla <davidme.news@usa.net>

Tue, 9 Feb 1999 12:20:21 +0100

According to the Spanish journal "El Pais", 5 Feb 1999 (quoting "Levante"), the Spanish bank Bancaja bought 1000 million pesetas (> 6 million euros) in shares of the Telepizza fast-food company, following a request for 1000 shares by a customer. It was a human error. The bank system was expected to detect transactions over 25 million pesetas but on the 4th of January, after switching to Euro-ready programs, this check was not enabled. The difference between the quantities bought and sold to the customer was held by the bank. Fortunately the value of the stock rose 30%.

David Mediavilla Ezquibela

⚡ E-Trade computers crash again -- and again

Edupage Editors <edupage@franklin.oit.unc.edu>

Sun, 07 Feb 1999 10:28:30 -0500

The computer system of online security firm E-Trade crashed on Friday for the third consecutive day. "It was just a software glitch. I think we were all frustrated by it," says an E-Trade executive. Industry analyst James Mark of Deutsche Bank is essentially sympathetic: "It's sort of a black eye for them. They've been claiming that their architecture is superior. But it's the application on a large scale. As soon as E-Trade's volumes started spiking up, they had the same problems as others." Marks adds: "If you call a broker, he may be on the phone or away from his desk or on vacation. There are all sorts of times you can't get through and once you put an order through there's no guarantee on terms. Here you have a customer base that is paying 5 percent to 10 percent of what it was paying for service in the full-commission environment and it's demanding service above what was available in the full-service environment. And they feel it's their right."
(*The Washington Post*, 6 Feb 1999; Edupage, 7 February 1999)

✶ Copier quota exceeded

Philip Koopman <koopman@cmu.edu>

Wed, 10 Feb 1999 20:11:47 GMT

We recently suffered temporary loss of copier privileges for my graduate course because we went over our quota. It seems the machine

says we made
4,294,967,026 copies in the last two weeks, and the caretakers
accepted it
as a correct number because it came from a computerized
accounting system (a
familiar RISK). They asked, with a straight face, what in the
world we had
been copying.

I tried pointing out that this is suspiciously close to 2^{32}
and that it is
far more likely the number -272 printed with an unsigned print
format, but
that argument didn't do me any good. I didn't waste time trying
to do the
page/minute calculation vs. elapsed wall time for them... So I
think the
fix is we'll reset the counter to zero and hope it doesn't
happen again.
And no, I have no idea how we got a negative number to start
with.

Phil Koopman -- koopman@cmu.edu -- <http://www.ece.cmu.edu/~koopman>

✶ Risks of Furbies: NSA was right! ([RISKS-20.14](#) and [.16](#))

Pete Mellor <pm@csr.city.ac.uk>
Wed, 10 Feb 1999 13:38:58 GMT

A friend of mine (Malcolm) related an alarming tale this
lunchtime.
He was helping a friend by driving her daughter to school. As
they
pulled up at the school gates, she took a Furby out of her bag.

"You'd better not take that to school." said Malcolm. "Leave it
in
the car." As he explained over lunch: "The worst decision I ever

made.

The <expletive deleted> thing talked to me all the way to the office."

As he pulled up in the office car park, his mobile 'phone rang. His secretary said "Where are you? Sam's been on the 'phone five times trying to get you. Weren't you supposed to be at that meeting?"

"<expletive deleted>" said Malcolm.

"<expletive deleted>" said the Furby.

As Malcolm said at lunch, "Well, at least it's going home with a slightly enhanced vocabulary!"

Risks to the US taxpayer: The NSA are spending a lot of their dollars stopping Furbies betraying how often <expletive deleted> is heard in top secret meetings.

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

[There are of course all sorts of potential covert-channel problems that NSA undoubtedly foresaw. One extreme example might be a normally inaccessible memory recording an entire day's worth of conversations that could later be unleashed by speaking an obscure unnatural-language secret phrase. A simpler example might be preprogrammed counters that merely tallied the frequency of occurrence of certain spoken keywords, which could subsequently be interrogated. PGN]

⚡ State of the states in Y2K readiness

Edupage Editors <edupage@franklin.oit.unc.edu>

Tue, 02 Feb 1999 15:05:09 -0500

A recent survey by the General Accounting Office shows only a third of the 421 computer systems used by the states to manage seven welfare programs are Y2K-compliant, with Medicaid the lowest at 16%. Systems that deal with child-care and child-welfare are about 50% compliant. An ongoing survey of state readiness conducted by the National Association of State Information Resource Executives (NASIRE) indicates that a narrow majority have completed repairs on more than half their critical systems and expect to finish the rest in the next few months. But the rest of the states are way behind, with Alaska in last place with only 15% of its computer systems repaired.

"For a state, if you're not ready, you're out of the game," says Steve

Kolodney, director of Washington state's information services and chairman

of NASIRE's year 2000 committee. It's estimated that states will spend

close to \$3.5 billion in bringing their computer systems to compliance, more

than half of the amount spent by the federal government to do the same.

(*Los Angeles Times*, 1 Feb 1999; Edupage, 2 February 1999)

⚡ The NT Blue Screen of Death

Bruce Wampler <bruce@objectcentral.com>

Wed, 10 Feb 1999 13:05:29 -0700

Submitted without any additional comment needed, taken from the MSDN Flash, Volume 3, Number 3, February 8, 1999 e-newsletter:

MSDN Flash Tips

MSDN Online Members-we have a new Tip for you each week at <http://msdn.microsoft.com/>

19) FORCE NT TO REBOOT AFTER A CRASH
From Exploring Windows NT

If you spend any time administering Windows NT, you're far too familiar with the Blue Screen of Death (BSOD) which displays the cause of the crash and gives some information about the state of the system when it crashed. The BSOD will sit on the screen until someone reboots the system, which could be very bad for a system that should be running 24 hours a day, like an Exchange server. You can force NT to automatically reboot after a crash by setting the value of HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\CrashControl\AutoReboot to 1. Once you've changed this value, NT will reboot after writing the crash log file.

Bruce E. Wampler, Ph.D. bruce@objectcentral.com <http://www.objectcentral.com>

⚡ The risks of "standard" software?

Rob Slade <rslade@sprint.ca>

Wed, 10 Feb 1999 13:31:58 -0800

I use the term "standard" here so as not to get into any arguments about "monopoly."

Most of the people in my wife's office use Microsoft Word as a word processor. (Not terribly surprising, I grant you.) They also use a number of other programs, some of them specialty programs for vertical markets.

The office has, up to now, standardized on 1 1/2" labels for most things, since almost all of the programs used had a setting for that format. Most of the labels have been printed by database programs, and not through the word processor.

Thus it was, that, until very recently, nobody realized that the new upgrade to Word (the entire office upgraded to Office 97 in May) did not have a setting for 1 1/2" labels, at least not "built in." And, having had some stock on hand for most of this year, it came as a shock when they recently submitted an order for 1 1/2" labels, and were told that the size was not available. At least, not in the generic house brand that they are used to ordering. Special label sizes can be ordered from a premium manufacturer like Avery, but are not available as house brands from any of the three main distributors that the office deals with.

When pressed, representatives for the companies all had the same story.

Nobody uses that size anymore, because Word doesn't use it. Therefore it is

no longer a standard size, and no longer a standard stock item.

rslade@vcn.bc.ca rslade@sprint.ca robertslade@usa.net
pl@canada.com

⚡ You are still in France

Adam Shostack <adam@netect.com>

Fri, 5 Feb 1999 12:02:52 -0500

In [RISKS-20.17](#), John Young reports on the French liberalization of crypto laws. Short-timers will remember the "You are now in France" attack mentioned in [RISKS-19.74](#). I am unable to find a patch for Windows that addresses this change, which means that people continue to be vulnerable because of a law now repealed. The risk, at a high level, is building vulnerabilities into software because of a law. The problems will survive long after the law is replaced.

⚡ It gets weirder every day...

Fred Cohen <fc@all.net>

Tue, 2 Feb 1999 18:18:44 -0800 (PST)

On two fronts... [relating to separate items from Fred in [RISKS-20.19](#)]

The error message from Windows was because the file named "sensitive countries" was read protected on the remote file server. The

error message

was simply confusing because it didn't identify that as a file name, but rather as the reason it stopped. The country it failed to process was indeed a 'sensitive' country (according to US policy today) so it took some time to figure out what really went wrong.

The PGP 'Trojan' is now being called a virus by folks who I believe wrote it (although they claim that they are not the authors, the set of things they know seems to suggest their authorship). They feel that it is illegal for those on the Internet to flood them with files and that they are going to suffer from denial of service. They brag that they have already gotten two sites that filled their FTP server with filenames shut off the Internet by ISPs and they threaten to get more shut off because they believe it is illegal to download files into their public write-only access area. They also assert that writing a virus is legal and that possessing unauthorized access control devices is legal... law enforcement seems to disagree.

My response has been rather less than generous. I have indicated that they could demonstrate their sincerity by:

- 1) disabling the remote ftp service for user anonymous with the password specified in the (now declared) virus.

- 2) Notifying all sites that have in the past and will in the future try to download to that address that they have the virus and provide instructions for mitigating the harm.

3) Providing all of the information required to track down the person who is receiving the information uploaded to that server and cooperating with local law enforcement to have them arrested.

To date, their (two of them so far) response has been less than positive, but I hope to convince them to do what they can to mitigate the harmful effects of this executable code regardless of their involvement.

Naturally, I also saw the DTK audit records of an attempted anonymous login against the ftp server port on one of the machines that somebody used to send a message to the named site at a time corresponding roughly to the time they sent the first e-mail on the subject.

Fred Cohen at Sandia National Laboratories at tel:925-294-2087
fax:925-294-1225

Fred Cohen & Associates: <http://all.net> - fc@all.net - tel/
fax:925-454-0171

[Fred's long disclaimer separating his two roles is omitted, as usual. PGN]

⚡ The risks of shopping at Amazon

Ross Anderson <Ross.Anderson@cl.cam.ac.uk>
Tue, 09 Feb 1999 10:15:12 +0000

Today I tried to order a book from Amazon. Their server asked for a credit-card number and I duly filled out the form. At the bottom it demanded a password. According to Amazon, this means that `you won't need to give us

your credit-card number again unless you enter a new shipping address'. I tried to enter the order without a password but it was refused.

What is the risk? Well, merchant retention of credit card numbers is a well known vulnerability; card numbers are much more likely to be stolen from merchant servers than while in transit on the net. Forcing customers to choose a password adds four extra risks. Firstly, the customer may choose a bad password; secondly, if he doesn't, he will probably write it down somewhere; thirdly, it will be kept on Amazon's system somewhere; and fourthly, it is likely to cause problems for people who have a dispute with their bank. I have acted as an expert witness in a number of court cases of disputed cash machine transactions, and the bank usually says 'you must have written the PIN down somewhere'. If everyone who shops at Amazon must choose a password which discloses their credit card details, then banks might turn away all complaints from people who've ever shopped there.

There's another problem, which neatly highlights the tension between the USA and Europe over data protection law. The Amazon server also refused my order when I refused to give them a telephone number. This isn't necessary for the transaction, so compelling disclosure is dubious under European law.

So I tried ordering from amazon.co.uk, which ought to abide by our local laws. This server also insisted on a password and a phone number, and even on a town in the address form (despite the fact that I live in the

countryside). It also didn't turn on SSL for the credit card capture form, so the card number was sent in clear. This is bad news, as we Brits don't have the benefit of US consumer protections: if my credit card number is stolen and abused, my bank will likely charge me the whole lot, and it's not clear what evidence I will have that it was Amazon's fault.

So amazon.co.uk appears to be in breach of the Data Protection Act of 1984. I therefore went to the Data Protection Registrar's Website at

<<http://www.dpr.gov.uk/>> and did a register search:

> Search terms: name=amazon and other=amazon.com

>

> No documents have been found that contain the above search terms.

> Please return to the form to begin a new search.

This looks highly illegal: under the Act, part 2, sections 5(1) and

5(5) compel everyone in the UK who holds personal data to register. (See <<http://www.hmsso.gov.uk/acts/acts1984/1984035.htm>>.)

I have e-mailed the Registrar, and will be interested to see what happens.

For several years now, the media have been hailing Amazon as the miracle of

the age, the model that all net based businesses - indeed all businesses

everywhere - should follow. I find that rather worrying,

Ross Anderson, Cambridge University

ross dot anderson at cl dot cam dot ac dot uk

✦ Re: Risks of successful security software ([RISKS-20.19](#))

Pete Mellor <pm@csr.city.ac.uk>

Tue, 2 Feb 1999 11:38:40 GMT

Nick Brown <Nick.BROWN@coe.fr> reported on the "hacker's revenge" story from the Daily Torygraph. There were one or two other interesting details, and the story as it appeared is a bit misleading.

At first glance, a reader might imagine that it was the "Access Denied" system that had been broken, which I think is not the case.

The challenge to the hackers to break their super firewall system was actually issued by the manufacturer, Gen Technology. Paul Smith (age 29) was described as **a** creator of Access Denied, not **the** creator. This implies that he was one member of the development team, and makes me wonder why he was personally singled out for retribution.

Gen Technology claim that over a period of several weeks, 240,000 attacks were made, but none breached the firewall. (How do they know the number of attacks, I wonder?) Apparently, the defensive features of Access Denied include checking a "user profile" and serial number on any computer seeking access, as well as the usual user name and password.

The vengeful hacker telephoned Mr. Smith, and said that he was part of a team of hackers (interesting in itself), and that he had been humiliated in front of his friends by being unable to fulfil his boast that he would get through the firewall in five minutes. There are fascinating clues to hacker

psychology here. He was described by Mr. Smith as having a "British voice". (Why is that so newsworthy, I wonder? Maybe to make it clear to foreigners that our crooks are just as clever as your crooks? :-)

Since, presumably, Paul Smith's personal credit records were not kept on the office machines at Gen Technology, the hacker must have attacked the records held by a central credit rating agency. This has alarming implications. If Paul Smith's credit rating can be falsified, then anybody could suffer the same fate. (It is probably not surprising that these agencies are sloppy about security, but it would seem that Paul Smith would have a prima facie case against them for negligence.)

Apparently, the hacker also described on the 'phone exactly what he was going to do. (In which case, why did Mr. Smith not alert the credit rating agency?) What the hacker apparently did was to insert six false "default notices" (as would result from persistent failure to keep up repayments on a credit card or loan, when you are deemed to have breached the terms of the contract) and one "County Court judgement" (an order to pay, made by a civil court in favour of a mortgage company when instalments are seriously in arrears, or of a local government authority when the defendant has not paid Council Tax). In the British system, the County Court judgement is the real killer when it comes to obtaining future credit.

(If the hacker would care to contact me in confidence, I might like a few things taken *off* my credit record! :-)

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: Government computer withholds benefits ... (R-20.19)

Pete Mellor <pm@csr.city.ac.uk>

Mon, 8 Feb 1999 11:16:50 GMT

The "Money Box" programme on BBC Radio 4 on Sat Jan 30 carried an item about problems with a UK government computer system which have led to underpayment of widows' pensions and other benefits.

The computer system involved is the new NIRS 2 system installed by the UK Government Department of Social Security (DSS), at a total cost of 140 million pounds sterling, which was said to be the largest civilian system in Europe.

The system was originally scheduled for completion in February 1997. The contractors now expect the remaining subsystems to be installed in March of this year. Problems have apparently been caused by "software bugs", although it was not clear from the programme to what extent software faults, as opposed to late and incomplete delivery, are responsible for the trouble.

NIRS 2 holds records of National Insurance (NI) contributions. (For non-UK readers, this is a form of tax, normally deducted at source along with

income tax, but shown as a separate deduction on salary advice slips. NI contributes to the government fund used to pay state pensions, unemployment benefit and sickness benefit.)

It appears that it has not been possible to input complete and up-to-date records of all National Insurance contributions, on which the amounts of certain benefits are calculated. This has forced benefits to be calculated by "guesswork" for more than one million claimants. One effect has been that women entitled to widow's benefit have been underpaid. Among those affected are 160,000 new pensioners, whose underpayment is 1.30 pounds per week *on average*, with some losing up to 100 pounds per week, for periods of up to two years.

The problems with NIRS 2 have also meant that the government has failed to pay a total of one billion pounds into private and occupational pension schemes.

There are a lot of angry widows beating on the doors of the Department of Social Security. So far, they have not received an awful lot of help. A short time ago, the Liberal Democrat MP David Rendell drew attention to the scandal by a question in Parliament. Steven Timms, Minister of State for Social Security, said in interview on the programme that, from the 6th January of this year, all *new* claimants would be paid correctly. He stated that the NI contribution records would be up-to-date by the end of March, and that existing beneficiaries whose total underpayment

exceeded 100 pounds, and whose payment due for lost interest exceeded 10 pounds, would automatically be reimbursed by lump sum payments for both underpaid benefits and interest.

This seems to be a continuation of the problem which surfaced in the middle of 1998, to which the DSS was reluctant to admit in case it led to a spate of fraudulent claims for unemployment benefit (since the payment offices could not check the bona fide of any claimant by going on-line to the system).

The government has set up a task force to deal with enquiries:-

NI Benefit Task Force, Benefits Agency Department ST, Quarry House,
Quarry Hill, Leeds LS2 7AU

Sources for the above are the Money Box programme itself (followed up by a 'phone call to Radio 4 enquiries), and their fact sheet. Anyone who requires further details should send a SAE to:-

Fact Sheet Week 5, Money Box, Room 6239, BBC Television Centre,
Wood Lane, Shepherds Bush, London W12 7RJ

Apparently, reports from current affairs programmes such as Money Box are not held on the BBC's Website, due to lack of staff to input them. However, a report also appeared in The Times on 26th January.

The National Audit Office report on National Insurance Fund Account 1997/98 is available on: www.open.gov.uk/nao

The fact sheet quotes two addresses and 'phone numbers

(available on request) from where hard copies of the NAO report may be ordered.

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

FMICS4 call for papers

Diego Latella <d.latella@cnuce.cnr.it>
Mon, 8 Feb 1999 14:36:22 +0100 (MET)

ERCIM

Working Group on Formal Methods for Industrial Critical
Systems

4th International Workshop on Formal Methods for Industrial
Critical Systems

Trento, Italy, July 11-12 1999

[http://www.cnuce.pi.cnr.it/cnuweb/research/resgroups/conc-meth/
FMICS/WS/Trento99/workshop.html](http://www.cnuce.pi.cnr.it/cnuweb/research/resgroups/conc-meth/FMICS/WS/Trento99/workshop.html)

[http://www.cnuce.pi.cnr.it/cnuweb/research/resgroups/conc-meth/
FMICS/WS/](http://www.cnuce.pi.cnr.it/cnuweb/research/resgroups/conc-meth/FMICS/WS/)

Trento99/workshop.html

Submission date 30 Mar 1999. Satellite meeting of FLoC'99
(<http://www.cs.bell-labs.com/cm/cs/what/floc99/>).

S. Gnesi, CNR-IEI, Via S. Maria 46, I56126 Pisa - ITALY phone:
+39 050 593489

REVIEW: "Mercury Rising", Douglas Pearson Ryne

Rob Slade <rslade@sprint.ca>
Fri, 5 Feb 1999 08:42:14 -0800

BKMERRIS.RVW 981113

"Mercury Rising", Douglas Pearson Ryne, 1998, 038002945

%A Douglas Pearson Ryne

%C 1350 Avenue of the Americas, New York, NY 10019

%D 1998

%G 038002945

%I Avon Books/The Hearst Corporation

%O +1-800-238-0658

%T "Mercury Rising"

Well, the other day I read "Mercury Rising." That's right, read, not watched. Actually, the movie was based on a book originally published as "Simple Simon," and, of course, the book was re-issued in conjunction with the movie release.

The book is about an autistic boy who, in the idiot savant way that sometimes comes with autism, is able to crack mathematically encrypted messages simply by looking at them. Unlikely? True. But I wouldn't want to bet against the abilities of organic computers. They can do some amazing things.

No, I'll stick to the computer and encryption stuff I know. It's hairy enough.

(By the way, I was amused to find out that Bruce Willis is Black.)

Let's start with the satellite. Now, this is a KH designation satellite, so no wonder it needs a crypto upgrade. Except, hold on a minute. The description of what it does doesn't have anything to do with spying or intelligence gathering. This is a plain, old, ordinary comsat, picking up

messages and relaying them. It doesn't need encryption capability any more than a piece of copper wire needs encryption: it just passes bits. The bits might be encrypted at source and decrypted at the destination, but that doesn't matter to the bits. In fact, if the message *isn't* encrypted at source, there is no point in encrypting it enroute.

But just suppose we do need encryption. OK, we'll send up the upgrade. Ready the command mode for reprogr... What? You're sending up a black box on the shuttle? And not just a tape, or anything: this is a module that is going to have to be swapped out for the box that is there?

Well, let's leave the satellite for the moment, shall we? Right, we have this new, super duper encryption algorithm. (Seems to be an awful lot like DES, what with S boxes and all. Hmmm. Seems to be even more like someone's misunderstood version of triple DES, but we'll let that pass.) (Has one heck of a key length, though. Wouldn't be very effective on short messages. Sorry, OK, back to the review.) Everybody is to use it. NSA, diplomatic corp, CIA, FBI, everybody. Same algorithm. Same crypto gear. Same key. Ummm, excuse me? (Good thing it's a long key, I guess. No, wait, that doesn't make any more sense...)

Right, let's move on to hackers. Now, of course, everyone who is any good at using computers is unhygienic. Or crippled. Or both. (This also applies to mathematicians, apparently.) And, of course, any evil hacker is completely undetectable as he slides down the T-1s of the

nation, slipping

into computers that have no connection to outside networks at all.

Especially one who is working for the government because he got caught doing this.

OK, I've believed enough impossible things before breakfast. If we have to get into white hat/black hat Illuminati, both groups completely occult, my brain is going to start to hurt.

copyright Robert M. Slade, 1998 BKMERRIS.RVW 981113
rslade@vcn.bc.ca rslade@sprint.ca robertslade@usa.net
pl@canada.com

Find virus, book info <http://victoria.tc.ca/techrev/rms.htm>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 21

Friday 12 February 1999

Contents

- [Memo on Y2K](#)
[via Dave Stringer-Calvert](#)
- [Y2K "fix" dates traffic offenses to 2097](#)
[Christopher Neufeld](#)
- [Computer fraud as another kind of Y2K risk?](#)
[Bruce Martin](#)
- [Judge moves to ban sale of self-help legal software in Texas](#)
[Doneel Edelson](#)
- [Risks of using power wiring for data traffic](#)
[Dan Pritts](#)
- [Hacking Web/FTP Servers](#)
[Ian Cargill](#)
- [CERT Advisory CA-99.03 - FTP-Buffer-Overflows](#)
[CERT](#)
- [Dangers of being the lowest price](#)
[Eytan Adar](#)
- ["Secure" fax](#)
[Steve Bellovin](#)
- [Our New Time Machine](#)
[Michael F. Hogsett](#)

- [Re: The NT Blue Screen of Death](#)
[Michael F. Hogsett](#)
 - [Re: The risks of "standard" software?](#)
[Michael F. Hogsett](#)
 - [Re: Programming Errors](#)
[Thomas J Gilg](#)
 - [REVIEW: "Fighting Computer Crime", Donn B. Parker](#)
[Rob Slade](#)
 - [REVIEW: "Intrusion Detection", Terry Escamilla](#)
[Rob Slade](#)
 - [SEPG `99 - 11th Software Engineering Process Group \(SEPG\) Conference](#)
[Carol Biesecker](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✉ **Memo on Y2K (source unidentified)**

Dave Stringer-Calvert <dave_sc@csl.sri.com>

Thu, 11 Feb 1999 11:46:49 -0800

Dear Boss:

I hope that I haven't misunderstood your instructions.
Because to be

honest, none of this Y to K problem makes any sense to me. At
any

rate I have finished the conversion of all of the months on
all the

company calendars for next year (year 2000). The calendars
have

returned from the printer and are ready to be distributed with
the

following new months:

Januark
Februark
Mak
Julk

I've also changed the following days:

Mondak
Tuesdak
Wednesdak
Thursdak
Fridak
Saturdak
Sundak

In general, all references to "Day" were changed to "Dak" (e.g. "President's Dak"). And all references to "Birthday" were changed to "Birthdak" (e.g. "Washington's Birthdak").

I had a hard time deciding about "New Year's Day", "Martin Luther King, Jr. Day", "Yom Kippur", and "Hanukkah", but I finally changed them to "New Year's Dak", "Martin Luther King, Jr. Dak", "Kom Yippur", and "Hanuyyah".

[1 April is still 1.5 months away, but it is never too early. However, I wish I could attribute this to its (unknown) author.

The pun on common parlance of using "i2j" for naming a transform from i to j is really delightful. PGN]

⚡ Y2K "fix" dates traffic offenses to 2097

Christopher Neufeld <neufeld@physics.utoronto.ca>

Fri, 12 Feb 1999 10:09:05 -0500 (EST)

In the Ottawa Citizen daily newspaper for Feb 12, 1999, an article appears about some Y2K silliness sending out notices of fines for traffic infractions. Notices of tickets issued in summer of 2097 went out, with warnings to pay before another date late in the twenty-first

century.

Estimates on the number of incorrect notices vary, from 207 across the province to 300 issued from a single court office.

Ministry of Attorney General spokesman Brendan Crawley is quoted as saying,

"It occurred on a production run while the company was working on making itself Y2K compatible." Further down in the article he is quoted as saying,

"It was just a matter of transposing every number 19 with the number 20, even when it wasn't right, and we've solved that problem."

One wonders how many companies are trying this particular windowing fix, in which no dates prior to Jan 1, 2000 can be represented. Putting the window in the year 2000 results in a rather severe discontinuity in the behaviour of the program, as it goes from being unable to represent any future dates to being unable to represent any past dates. I'm also led to wonder how many other companies are making and testing partial fixes on production equipment. I am not particularly comforted by the assurance that the particular problem leading to these erroneous notices has been solved.

Christopher Neufeld <neufeld@physics.utoronto.ca>

<http://caliban.physics.utoronto.ca/neufeld/Intro.html>

⚡ Computer fraud as another kind of Y2K risk?

<Bruce_Martin@manulife.com>

Thu, 11 Feb 1999 12:35:44 -0500

Perhaps I've been reading too many Bruce Sterling novels, but it occurs to me as I listen to various Y2K scenarios that no one has addressed the very real possibility of computer fraud timed to coincide with the Year 2000.

Consider: The great majority of physical thefts are perpetrated under circumstances that favour the anonymity of the thief. The morning of 1 Jan 2000 is widely predicted to be chaotic. Random losses of wealth are not only possible but actually expected by many. (Certainly few insurance companies would be willing to underwrite such losses.)

Consider also: In preparation for Y2K, virtually all major wealth-bearing organizations are hiring vast teams of consultants to write and re-write the billions of lines of code their wealth depends on. Most of these consultants have never worked for their respective clients before, and many cannot expect to do so again once the Y2K crisis has passed.

It should not be difficult for a lone, less-than-scrupulous consultant to salt this sea of new and re-written code with just a few extra lines ...and as a result redirect a significant fraction of an organization's wealth to a blind account in the Cayman Islands at the stroke of midnight on 31 Dec 1999.

Who can prevent this? Likely not corporate auditors, too occupied with the question of their systems' integrity to consider their consultants' integrity. The possibility of recovering the missing funds will also be

greatly diminished in post-Y2K confusion ("Hey, we were *expecting* losses, weren't we?"). In any event, the world is full of countries willing to protect the anonymity of a new multi-millionaire immigrant.

And so we have motive, opportunity and a diminished likelihood of retribution. It seems to me that the countdown to this sort of crime is already underway.

Bruce Martin, Toronto

⚡ Judge moves to ban sale of self-help legal software in Texas

"Edelson, Doneel" <doneeledelson@aciins.com>

Wed, 3 Feb 1999 17:09:10 -0500

Judge moves to ban sale of self-help legal software in Texas; Use of software is called unlicensed practice of law [AP item, 2 Feb 1999]

U.S. District Judge Barefoot Sanders is moving to ban the sale of self-help legal software such as Quicken Family Lawyer. Ralph Warner of Nolo Press said he considered this a step 20 years back into the past. [PGN Very Stark Abstracting]

[Judge the Quicken the Dead? PGN]

⚡ Risks of using power wiring for data traffic

Dan Pritts <danno@ans.net>

Thu, 11 Feb 1999 13:57:45 -0500

<http://cgi.sjmercury.com/premium/front/docs/devilphonel1.htm>

Summary: cable TV decoder that calls in every night to record pay-per-view, combined with "wireless jacks" that send phone traffic across house power wiring, seem to have given San Jose family a \$500 phone bill for calls made by someone else.

dan pritts, ans systems engineering, ann arbor, MI uunet
worldcom 734-214-7409

⚡ Hacking Web/FTP Servers

Ian Cargill <ian@soliton.demon.co.uk>

Fri, 12 Feb 1999 16:45:18 +0000

There have been many press items recently about FTP and Web servers being hacked. Indeed, [RISKS-20.18](#) had a couple of submissions about hacked software with Trojans/Trapdoors being placed on servers. This is **so** common, that I find it strange that there doesn't seem to be much demand for what I would see as a good - though not complete - solution; write-protectable hard drives.

Surely it would be very easy for HD manufacturers to produce drives with a **physical** 'off' switch which made it impossible to write to a drive unless you had physical access to the server. You would prepare updates 'off-line', switch the server drive to 'writable', update all the necessary files, then switch the drive back to 'write protected'. A second, 'normal'

drive could be used to dynamically created pages.

I would have thought this easy, practical and going a long way to solving the problem. The seeming absence of any such drives suggests to me that I must be wrong. Can anyone explain to me why such a scheme would be impractical or unworkable?

Ian Cargill CEng MIEE, Soliton Software Ltd.

🔥 CERT Advisory CA-99.03 - FTP-Buffer-Overflows

CERT Advisory <cert-advisory@cert.org>

Thu, 11 Feb 1999 18:11:43 -0500

[RISKS does not generally include CERT Advisories, because we assume those needing to know are already receiving them. This one is excerpted, in light of Steve Bellovin's comments at several

recent meetings to the effect that 8 out of the 13 CERT Advisories

issued during 1998 involved security vulnerabilities caused by buffer overflows. That alarming ratio deserves greater attention.

Here is one for 1999, affecting many different platforms. PGN]

CERT Advisory CA-99-03-FTP-Buffer-Overflows

Original issue date: February 11, 1999

Topic: Remote buffer overflows in various FTP servers leads to potential root compromise.

Source: Netect, Inc.

To aid in the wide distribution of essential security information, the

CERT Coordination Center is forwarding the following

information from

Netect, Inc. Netect, Inc. urges you to act on this information as soon

as possible. See Appendix C for Netect, Inc. contact information.

Please contact them if you have any questions or need further information. [... <<http://www.netect.com/>>]

[The entire advisory is available from:

<http://www.cert.org/advisories/CA-99-03-FTP-Buffer-Overflows.html>]

⚡ Dangers of being the lowest price

Eytan Adar <adar@parc.xerox.com>

Mon, 8 Feb 1999 17:31:12 PST

An interesting article appeared today on Wired's on-line site (<http://www.wired.com/news/news/business/story/17803.html>).

Apparently,

Buy.com made a mistake in its pricing of a Hitachi monitor and listed it as \$164.50. This monitor was in fact \$588.

So 48 hours later, and with 1600 monitors purchased, Buy.com has a public relations nightmare on its hands. The cost of this "typo" will be around \$320,000 if Buy.com actually fulfills the order.

Aside from the obvious questions like, why they didn't notice a sudden blow up in orders for this monitor?, there is an interesting issue regarding Buy.com's policy of being the lowest price on the net.

My understanding, and I could be wrong about this, is that Buy.com actually has (ro)bots (automated agents) roving the net looking for

cheaper prices.

If they find a cheaper price the price automatically gets dropped on their site. Even if the process isn't driven by a bot but by a human I think the risk is still valid...

Now I can't say for sure that this is what happened, but you can see the obvious danger here. A retailer (that Buy.com competes with) somewhere on the net may have made its own mistake. The bot, not knowing any better, would have carried that price back to Buy.com. The other alternative, of course, is that someone could maliciously have set the price low. Either way, the "price virus" gets transmitted by an ignorant bot back to parent site, and we're back to our public relations nightmare.

e-commerce... gotta love it...

Eytan Adar

[If you are not careful, you just bot the farm. PGN]

✶ "Secure" fax

Steve Bellovin <smb@research.att.com>

Thu, 11 Feb 1999 12:03:55 -0500

The 15 Feb 1999 issue of **Newsweek** describes an Internet-based fax product.

You sign up with them and get a 10-digit phone number; faxes to that number are emailed to you. This is described by **Newsweek** as good for confidential faxes, since it bypasses the company fax machine. There's no mention about the risks of sending confidential information

through a third party.

Trying to learn how this company protects your information is itself a bit amusing, since *Newsweek* may have gotten the name wrong. In the on-line version at least, it's listed as www.e-fax.com, a site that is apparently under construction. Did *Newsweek* mean www.efax.com, which offers a similar service? Its pages demand a careful read-through on the subject of security. Among other things, one learns that faxes are "protected" by a password -- they seem to avoid the word "encrypted", which may be a clue. And even that level of protection is only available if you use their viewer on a (of course) Windows platform; users of other systems (whose existence they at least acknowledge the existence of!) are sent unprotected TIFF files. There's no mention of anything like PGP.

I should note that at least in the press releases accessible via the e-fax Web site, they make no claims about the superiority of their product for confidential material. That seems to be *Newsweek*'s spin. Efax does promise to be careful with your data, though.

One more risk -- it takes a lot of wading through the fine print of the privacy policy to realize that you're signing up to receive electronic junk mail. This is apparently an advertising-supported service, which is not in itself wrong or evil -- they should just say so in a more upfront fashion.

Steve Bellovin

⚡ Our New Time Machine

"Michael F. Hogsett" <hogsett@csl.sri.com>

Thu, 11 Feb 1999 12:26:06 -0800

It appears as though our new switch / router doubles as a time machine.

I was performing a few tests, one of which was a flood ping. The minimum round-trip time has been consistently negative...

It is either sending ICMP replies from the future or anticipating them...

```
# ping -f 192.168.1.10
PING 192.168.1.1 (192.168.1.10): 56 data bytes
.....
--- 192.168.1.10 ping statistics ---
2583 packets transmitted, 2568 packets received, 0% packet loss
round-trip min/avg/max = -8.0/1.9/7.1 ms
```

(Well, OK, the most likely thing is that there is a bug in the ping program under Linux...)

Mike

[Note: The IP address has been altered to protect the innocent. PGN]

⚡ Re: The NT Blue Screen of Death ([RISKS-20.20](#))

"Michael F. Hogsett" <hogsett@csl.sri.com>

Thu, 11 Feb 1999 09:48:27 -0800

```
> HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\CrashControl
\AutoReboot to 1.
> Once you've changed this value, NT will reboot after writing
the crash log
> file.
```

Assuming of course that the crash did not corrupt the data structure storing the 1, replacing it with an invalid value.

Michael Hogsett

⚡ Re: The risks of "standard" software? ([RISKS-20.20](#))

"Michael F. Hogsett" <hogsett@csl.sri.com>

Thu, 11 Feb 1999 09:52:15 -0800

```
> Nobody uses that size anymore, because Word doesn't use it.
Therefore it is
> no longer a standard size, and no longer a standard stock item.
```

So assume that if Word no longer prints onto 8.5 x 11" paper that the entire industry will stop producing it.

Michael Hogsett

⚡ Re: Programming Errors (Gilham, [RISKS-20.18](#))

"GILG,THOMAS J (HP-Corvallis,ex1)" <Thomas_Gilg@ex.cv.hp.com>

Mon, 8 Feb 1999 13:46:49 -0800

```
> [...] In two days he has reports three
> instances of the following common C error:
>   if (x = y)           instead of           if (x == y)
```

Sorry, but another common C error is to assume the above.

Consider

if the intent of the expression was:

```
if ( pChar = pMyString ) {  
    // increment pChar through my string looking for tokens  
    .....  
}
```

Granted the more visually obvious coding style would have been:

```
if (pMyString) {  
    pChar = pMyString  
    // increment pChar through the string looking for tokens  
    .....  
}
```

Thomas Gilg <tomg@cv.hp.com>

⚡ REVIEW: "Fighting Computer Crime", Donn B. Parker

Rob Slade <rslade@sprint.ca>

Wed, 10 Feb 1999 12:19:41 -0800

BKFICMCR.RVW 981106

"Fighting Computer Crime", Donn B. Parker, 1998, 0-471-16378-3,
U\$34.99/C\$49.50

%A Donn B. Parker dparker@sric.sri.com

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 1998

%G 0-471-16378-3

%I John Wiley & Sons, Inc.

%O U\$34.99/C\$49.50 416-236-4433 fax: 416-236-4448

rlangloi@wiley.com

%P 512 p.

%T "Fighting Computer Crime: A New Framework for Protecting
Information"

Parker feels that too much of the data security field concentrates on technical answers to the problems of reliability, integrity, and availability of data, and doesn't pay sufficient attention to those people who are deliberately out to read, steal, or ruin your information and systems. Personally, I find it rather ironic that he defines "crimoids," in chapter one, as minor events promoted to much higher significance by the media, and public misperceptions. In the non-specialist realm, more people spend more time worrying about "hackers" than ever back up their drives. (I am reminded of a friend; an intelligent and educated person who started his career programming large and sophisticated information systems and who has now risen to the executive ranks; who has for years refused to get a modem for his home computer. In spite of his frequently expressed desire for access to the Internet, and my repeated assurances that with his current computer and operating system there is no hidden danger, he remains convinced that the mere attachment of a modem to his machine will allow someone to break into his computer and damage it.)

Who, then, is this book written for? The author does not say, but what he does say in the preface seems to indicate that he is not writing for those whose business cards make reference to security. (I have neither argument nor inclination to dispute Parker's assertion that security "professionals" do not really deserve the designation.) But if this text is aimed at the general public, chapter one's emphasis on the dangers and lack of protection

would seem more inclined to incite further panic, rather than a realistic and measured response.

Chapter two is an interesting and useful examination of an often unasked question in the field: what is the nature of the information we are supposedly securing? There are valuable side points, such as both the danger and the opportunity in the security arena presented by the Year 2000 problem. At the same time, I have to note that an erroneous description of the Cascade virus is an example of Parker's asserting points that are just beyond the available facts, and, for me anyway, has an unfortunate effect on the trustworthiness of the work as a whole. The review of cybercrime, in chapter three, has more reference to journalism and other forms of fiction than to reality, but I have to agree with everything said there. Computer misuse and abuse is discussed in chapter four. (As if to make up for chapter two, the section on viruses is very good.) Network misuse is covered in chapter five, and although I still have trouble believing in the reality of salami attacks (Parker's sole example is said to have resulted in a conviction, but no citation is given) I am a bit more willing to accept his broader definition. Chapter six is extremely strong in portraying a realistic and broadly based analysis of characteristics of computer criminals. A similarly informed and balanced approach distinguishes chapter seven, regarding hacker culture, but there is also a universally condemnatory tone that is not wholly justified by the facts as presented.

Chapter eight is a very helpful first step for those wanting to deal in the art of computer security.

Chapter nine reviews the deficiencies in most current security practices, noting overprotection in some areas while ignoring loopholes in others, and a flowery jargon that serves mostly to hide the fact that security people just don't feel very comfortable with what is going on. However, Parker's new model of security, in chapter ten, while it is very clear and useful, does not extend recent work in, say, electronic commerce. On the one hand, this congruence does support the model, but on the other, one can't really say it is too novel. The popular, but demonstrably incomplete, risk assessment study is de-emphasized in favour of a more difficult, but more realistic, baseline security standard in chapter eleven. Details on how to conduct such a study are very helpfully given in chapter twelve, although the benchmark chart is going to be much harder to come by than is made clear in the text. Chapter thirteen provides a practical and useful set of criteria for determining control objectives. A number of security tactics are detailed in chapter fourteen. Chapter fifteen takes the larger strategic view. (I was delighted to see the inclusion of a section on corporate ethics in this chapter. Recently I contracted to produce a security document for an educational institution, and was told to take the section on ethics out.) Management of security, in chapter sixteen, includes provisions for training, policy, and other factors.

Chapter

seventeen finishes off with a look to the future. The material, while thought-provoking, is possibly more likely to generate arguments than solutions.

Parker's stance on security in general definitely puts him in the camp of the professional paranoids. However, absent the first and last chapters, there is a lot of good, solid knowledge here to help educate any security practitioner. The material in the second half of the book is just as valuable to the security process as the more technical works such as "Practical UNIX and Internet Security" (cf. BKPRUISC.RVW) by Spafford and Garfinkel, albeit in quite a different way. An informed security policy is every bit as important as a good set of "access" controls.

copyright Robert M. Slade, 1998 BKFICMCR.RVW 981106
rslade@vcn.bc.ca rslade@sprint.ca robertslade@usa.net
pl@canada.com

REVIEW: "Intrusion Detection", Terry Escamilla

Rob Slade <rslade@sprint.ca>
Fri, 12 Feb 1999 08:33:14 -0800

BKINTRDT.RVW 990108

"Intrusion Detection", Terry Escamilla, 1998, 0-471-29000-9,
U\$39.99/C\$56.50

%A Terry Escamilla

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 1998

%G 0-471-29000-9

%I John Wiley & Sons, Inc.
%O U\$39.99/C\$56.50 416-236-4433 fax: 416-236-4448
rlangloi@wiley.com
%P 348 p.
%T "Intrusion Detection: Network Security Beyond the Firewall"

Maybe my perception is skewed from having been involved with physical security as well as the computer kind, but I see intrusion detection as being part of security. There is no security system that cannot be penetrated or bypassed, and so detection is, in my view, simply a fact of security life. Isn't that what auditing, one of the main pillars of data security, all about? So I find the attempt to sell the idea of intrusion detection somewhat redundant. Then there is the emphasis on reviewing commercial Intrusion Detection Systems (IDS).

Part one looks at what happens before intrusion detection: the traditional role and model of computer security. Chapter one provides a brief, but reasonably sound, overview of this classic paradigm, concentrating on defining most of the theoretical terms used. Some identification and authentication details from both UNIX and Windows NT start our chapter two, which then meanders through a few examples of password cracking, and finally ends with a look at ticket granting systems and other authentication improvements. A similar look at access control is provided by chapter three. Given the complexity of networking and network security, the number of topics covered in chapter four is unsurprising.

Part two looks at intrusion detection by extending the traditional security design. Chapter five is fairly pivotal, as evidenced

by the title "Intrusion Detection and Why You Need It." The "why" part comes first, with a rather weak example showing that security systems can have loopholes if you don't configure or program everything properly. Intrusion detection then seems to be defined as the usual game of find vulnerability-fix-repeat, only in automated form. A number of possible attacks are mentioned in chapter six, and then a promotion of the addition of an IDS layer to a system, without a corresponding reiteration of the warning, from chapter four, that layers in a system increase the possibility of loopholes. I was rather astonished that SATAN [Security Administrator's Tool for Analyzing Networks] was not included with the vulnerability scanners mentioned in chapter seven. Two more sophisticated products are reviewed in chapter eight. Chapter nine looks at the possibility of catching intruders by traffic analysis, although "catch" seems to be too strong a term to use here. Since most of the foregoing deals with UNIX, chapter ten looks at similar products for NT, although most of the material seems to concentrate on NT's own audit logs.

Part three looks at dealing with an intrusion once you have detected it. Chapter eleven recommends being prepared well, detecting early, analyzing thoroughly, and deciding judiciously. In one useful piece of advice, it recommends against an attack on a system you may think is hitting on yours. Chapter twelve is a quick summary of the book.

As the author admits, in the final chapter, that intrusion detection

systems are not the final word in computer security, I am inescapably reminded of the battles in the antiviral field over the relative strengths of scanners, activity monitors, and change detection systems. What works best? A combination approach, of course. The price of a secure system is more budget for administration time and tools. This book does not present any radically new approach or technique for system security. In fact, with the emphasis on proprietary commercial products, the work will date quite quickly. For those who are looking to add an automated IDS to their current network, the volume could act as a kind of incomplete buyer's guide.

copyright Robert M. Slade, 1999 BKINTRDT.RVW 990108
rslade@vcn.bc.ca rslade@sprint.ca robertslade@usa.net
pl@canada.com

SEPG `99 - 11th Software Engineering Process Group (SEPG) Conference

Carol Biesecker <cb@SEI.CMU.EDU>
10 Feb 1999 20:14:55 GMT

SEPG `99 - The 11th Software Engineering Process Group (SEPG) Conference

Theme: Software Process Improvement (SPI) Investments Today for a Changing Tomorrow

March 8-11, 1999

Hyatt Regency Atlanta, Atlanta, Georgia

For complete details, including the preliminary program, and registration information, visit the SEI Web site at:

<http://www.sei.cmu.edu/products/events/sepg/>

Customer Relations

Software Engineering Institute

Carnegie Mellon University

Pittsburgh, PA 15213-3890

Phone, Voicemail, and On-Demand FAX: 412 / 268-5800

E-mail: customer-relations@sei.cmu.edu

World Wide Web: <http://www.sei.cmu.edu/products/events/sepg/>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 22

Saturday 20 February 1999

Contents

- [Process-table attack](#)
[Simson L. Garfinkel](#)
- [Store Baelte Bridge not Y2K safe](#)
[Debora Weber-Wulff](#)
- [More risks of "training" on live systems](#)
[Dave Stringer-Calvert](#)
- [A franglais booboo](#)
[Vicky Larmour](#)
- [Cellphone risks in flight again?](#)
[Chuck Weinstock](#)
- [Re: "Page-layout program hazards" and...](#)
[Mark Brader](#)
- [Re: Programming Errors](#)
[Thomas J Gilg](#)
- [The risks of on-off switches?](#)
[Elliott Potter](#)
- [Re: Hacking Web/FTP Servers](#)
[Andy Goldstein](#)
[Rob Slade](#)
[Nigel Rantor](#)

- [Re: Computer fraud as another kind of Y2K risk?](#)
 - [Chuck Karish](#)
 - [Dorothy Denning](#)
 - [Win Treese](#)
 - [8th USENIX Security Symposium: papers due March 9](#)
 - [Jennifer Radtke](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Process-table attack

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

Fri, 19 Feb 1999 16:08:06 -0500

Wide-ranging attack works against almost any UNIX systems on the Internet

ABSTRACT:

The Process Table Attack is a [relatively] new kind of denial-of-service attack that can be waged against numerous network services on a variety of different UNIX systems. The attack is launched against network services which fork() or otherwise allocate a new process for each incoming TCP/IP connection. Although the standard UNIX operating system places limits on the number of processes that any one user may launch, there are no limits on the number of processes that the superuser can create other than the hard limits imposed by the operating system. Since incoming TCP/IP connections are usually handled by servers that run as root, it is possible to completely fill a target machine's process table with multiple instantiations of network servers. Properly executed, this attack prevents

any other command from being executed on the target machine.

DETAILS

In the book *Practical UNIX and Internet Security*, Gene Spafford and I observed that the UNIX operating system originally contained few defenses to protect it from a denial-of-service attack. This is changing. With the growth of the Internet, there has been a concerted effort in recent years to strengthen the operating system and its network services to these attacks.

Each time a network client makes a connection to a network server, a number of resources on the server are consumed. The most important resources consumed are memory, disk space, and CPU time. Some network services, such as sendmail, now monitor system resources and will not accept incoming network connections if accepting them would place the system in jeopardy.

One system resource that has escaped monitoring is the number of processes that are currently running on a computer. Most versions of UNIX will only allow a certain number of processes to be running at one time. Each process takes up a slot in the system's process table. By filling this table, it is possible to prevent the operating system from creating new processes, even when other resources (such as memory, disk space, and CPU time) are widely available.

The implementation of many network services leaves them open to a process table attack ? that is, an attack in which the attacker fills up

the target computer's process table so that no new programs can be executed. The design of some network protocols actually leads the programmer into making these mistakes.

An example of such a protocol is the finger protocol (TCP port 79). The protocol follows this sequence:

1. The client makes a connection to the server.
2. The server accepts the connection, and creates a process to service the request.
3. The client sends a single line to the server consisting of the name of the entity that the client wishes to finger.
4. The server performs the necessary database lookup and sends the information back to the client.
5. The server closes the connection.

To launch a process table attack, the client need only open a connection to the server and not send any information. As long as the client holds the connection open, the server's process will occupy a slot in the server's process table.

On most computers, finger is launched by inetd. The authors of inetd placed several checks into the program's source code which must be bypassed in order to initiate a successful process attack. If the inetd receives more than 40 connections to a particular service within 1 minute, that service is disabled for 10 minutes. The purpose of these checks was not to protect the server against a process table attack, but to protect the server against

buggy code that might create many connections in rapid-fire sequence.

To launch a successful process table attack against a computer running `inetd` and `finger`, the following sequence may be followed:

1. Open a connection to the target's finger port.
2. Wait for 4 seconds.
3. Repeat steps 1-2.

The attack program is not without technical difficulty. Many systems limit the number TCP connections that may be initiated by a single process. Thus, it may be necessary to launch the attack from multiple processes, perhaps running on multiple computers.

We have tested a variety of network services on a variety of operating systems. We believe that the UW `imap` and `sendmail` servers are also vulnerable. The UW `imap` contains no checks for rapid-fire connections. Thus, it is possible to shut down a computer by opening multiple connections to the `imap` server in rapid succession. With `sendmail` the situation is reversed. Normally, `sendmail` will not accept connections after the system load has jumped above a predefined level. Thus, to initiate a successful `sendmail` attack it is necessary to open the connections very slowly, so that the process table keeps growing in size while the system load remains more or less constant.

We have also seen a variety of problems on BSD-based machines being used as the attacker. When the target machine freezes or crashes, the attacker

machine sometimes crashes as well. Apparently the TCP stack does not gracefully handle hundreds of connections to the same port on the same machine simultaneously going into the FIN_WAIT_2 state.

There are variants of this attack:

1. Use IP spoofing so that the incoming connections appear to come from many different locations on the Internet. This makes tracking considerably harder to do.
2. Begin the attack by sending 50 requests in rapid fire to the telnet, rlogin and rsh ports on the target machine. This will cause inetd to shut down those services on the target machine, which will deny administrative access during the attack.
3. Instead of initiating a new connection every 4 seconds, initiate one every minute or so. The attack slowly builds, making it more difficult to detect on packet traces.

There are several ways to defend against the attack:

1. inetd and other programs should check to see the number of free slots in the process table before accepting new connections. If there is less than a predefined number of free slots, new connections should be accepted.
2. Alternatively, if there are more than a preset number of network daemons for the service running, incoming requests should be queued rather than serviced.
3. Network services (such as finger) should implement timeouts. For example, the statement alarm(30) could be inserted into the

finger

daemon source code so that the program would stop running after 30 seconds of execution.

Simson L. Garfinkel, Sandstorm Enterprises, Inc. <www.sandstorm.net>

[Simson informed me over a year ago that he had discovered this attack

and had notified many relevant operating system vendors. To the best of

my knowledge, no one has addressed the problem in the intervening year.

We thus include this item in the hopes of spurring some action, or at

least awareness and public discussion. On the other hand, we of course

do not recommend conducting experiments to demonstrate this flaw on

other people's systems. PGN]

⚡ Store Baelt Bridge not Y2K safe

Debora Weber-Wulff <Debora.Weber_Wulff@te.mah.se>

Mon, 15 Feb 1999 12:48:26 +0100

A small article in Syssvenskan from 1999-02-15 notes that the new bridge in

Denmark over the Store Baelt (which was just opened last year) is not Y2K

safe. Tests have shown that approx. 50% of all the systems involved

(signalling, signs, etc) will have some problem or other on 2000-01-01. But

that is not a problem, it just means that some of the trains will not be

able to cross the bridge. [I hear PGN already: We'll cross that bridge when

we come to it!]

Debora Weber-Wulff MALMOe HOeGSKOLA 205 06 Malmo SWEDEN
+46-40-6657254 Debora.Weber_Wulff@te.mah.se <http://www.te.mah.se/person/dw/>

[Debora may be growing too big for her bridges by preempting PGN. PGN]

⚡ More risks of "training" on live systems

Dave Stringer-Calvert <dave_sc@csl.sri.com>

Fri, 12 Feb 1999 18:39:48 -0800

Palo Altans watching the city's Web site yesterday morning got a bit of a shock when a warning message told them Matadero Creek was half full, and Adobe Creek was close to spilling over. The messages popped up on home computer screens because Public Works staffers holding a training session tweaked the city's creek monitoring system as part of a demonstration. In reality, it was a sunny morning and the creeks were nowhere near overflowing. [Excerpt from "Creek Web Site Snafu Causes Alarm in P.A." by Elaine Goodman, *Palo Alto Daily News*, 12 Feb 1999]

The creek level Web site can be accessed from
www.city.palo-alto.ca.us/emergency/emergency.html
Follow the link to "creek monitoring devices."

[The nicest quote in the article was Elaine's:

"Residents flooded City Hall with calls to see what was going on."

Water you waiting for? PGN]

⚡ A franglais booboo

Vicky Larmour <vicky.larmour@camcon.co.uk>

Wed, 17 Feb 1999 13:04:24 +0000

Someone on a local newsgroup noticed the following text in a promotional leaflet for a local health and fitness centre:

> The brassiere is the perfect environment for
> a chat over coffee or a light lunch after exercise.

I saw this and immediately thought "Spelling checker" and sure enough, "brasserie" is not recognised in Word's spelling checker and the suggested replacement is "brassiere". Seems like there's a risk of major embarrassment here.

Vicky Larmour, Software Engineer, Cambridge Consultants Ltd,
Cambridge, UK

[Au contraire! It probably brought in a lot of new customers. Too bad

Webster could not have been a Web-ster. He would have enjoyed it. PGN]

⚡ Cellphone risks in flight again?

Chuck Weinstock <weinstoc@SEI.CMU.EDU>

Thu, 18 Feb 99 09:28:17 EST

Investigations are proceeding on the Thai Airways Flight TG261 jet that crashed in December 1998 in southern Thailand. Pilots had attempted a landing despite orders to divert to another airport after two unsuccessful

approaches during a storm. The airport's instrument landing system was inoperative. There is also an unofficial report that mobile-phone calls from passengers are being studied to see whether they might have interfered with the plane's controls. [Source: Mobile phones may have caused Thai Airways crash: report, 18 Feb 1999, from C-afp@clari.net (AFP), PGN Abstracting]

✈ Re: "Page-layout program hazards" and... (Byrd, [RISKS-20.18](#))

Mark Brader <msbrader@interlog.com>
Tue, 16 Feb 1999 15:06:26 -0500 (EST)

> ... A much simpler solution ... would simply be for TROFF to
> report any illegal commands it encountered ...

The basic problem here is that just as in C the unlikely construct "if(x=y)" is a legal one, so ".garbage" or "'garbage" is legal in troff. It is a defined feature of the language that macros are invoked in the same way as requests (commands), and that invocation of an unknown macro is permissible and does nothing.

troff is not usually used alone, but with a macro package whose details are unknown to the user. That feature allows the designers of macro packages to provide hooks: by calling an otherwise unknown macro at a certain time, they allow the user to define an action that will occur at that time. The same construct might also be used internally within a macro

package,
e.g. to write out a footnote if there is one pending.

Several newer versions of troff, including the one that I used to maintain for SoftQuad, do provide an option to issue a warning on invocation of an unknown macro. But for the backward compatibility reason that I've just explained, for at least some users this can't be the default behavior.

Even this warning might not always be sufficient, because a user who doesn't know that ' is special might also accidentally invoke a real request or macro. This is particularly true with the original troff syntax, where a command line like .trash or 'trash (in this case the two are equivalent) would be taken as .tr ash (i.e. the first two letters taken as the command, and the rest the argument). That particular command introduces character transliteration and would turn these words into "T st psrticularr commsnd introduces c srscter trnsliterstion snd would turn t ese words into".

troff *is* a tricky language to use, and this is not easily changed.

Mark Brader, Toronto, msbrader@interlog.com

✶ Re: Programming Errors (Gilham, [RISKS-20.18](#))

"GILG,THOMAS J (HP-Corvallis,ex1)" <Thomas_Gilg@ex.cv.hp.com>
Tue, 16 Feb 1999 10:49:52 -0800

[We received a large number of comments on this. I chose to include only Thomas's blanket response to all who cc:ed him, hoping that does not invite even further responses. PGN]

We all started with:

```
> if ( pChar = pMyString )
```

Thomas Gilg wrote:

```
> Granted the more visually obvious coding style would have been:
```

```
>
```

```
> if (pMyString) {  
>     pChar = pMyString
```

Pascal and others generally wrote:

```
> Which, of course, is wrong. It's actually equivalent to:
```

```
>
```

```
> pChar = pMyString;  
> if (pChar) {
```

Pascal's form is indeed the "language" equivalent - the assignment is first and then the comparison.

I knowingly constructed (assumed ;-)) my form to be an "intent" equivalent.

Having worked with most of the major UNIX vendors on X-Windows and the Common Desktop Environment (CDE), and having been the architect and coder for several now-standard portions of each, I was trying to recall the intent I had seen most often among the companies.

On a related note. While most of us are used to constants appearing on the right, I've also seen where many people (not me) deliberately place constants on the left side of an intended '==':

```
if (NULL == pChar)
```

While it looks weird, it does help catch '=' typos via the

assignment of
something to a constant; ex, NULL = pChar.

While on the topic - the original note also mentioned 'case' statements without 'break's. I'm 99% sure that such situations occur in the CDE code, but once again it was intended. In this case, I doubt even coding style could help convey the intent, so hopefully there are comments!

All in all, my own mistrust of self documenting code probably explains why a statistic generated by the CDE 2.0 partners (SUN, IBM and HP to name a few) revealed that the most heavily commented libraries and executables in all of CDE were written by me, and they weren't all // tomg XXX comments ;-)

Thomas Gilg <tomg@cv.hp.com>

⚡ The risks of on-off switches?

Elliott Potter <epotter@abraxis.com>

Sun, 14 Feb 1999 22:16:42 -0500

> Surely it would be very easy for HD manufacturers to produce drives with a
> *physical* 'off' switch which made it impossible to write to a drive unless
> you had physical access to the server. ...

This reminds me of a problem we encountered when I worked the PC Helpdesk at ACS. I came in to work one morning and there was another member of the Helpdesk there, staring at two brand-new inoperational ThinkPads...they couldn't get them to turn on. He grabbed a battery that had

arrived with a package of replacement batteries the day before and had been charging in a laptop...plugged it in to the new one, and the same thing--nothing. He grabbed an old battery, plugged it in, and it worked fine. As he was about to re-package the batteries and send them back, I noticed a "I O" marking on one--turns out that the batteries had an on-off switch, and the new ones had arrived switched off. No one there had ever heard about this one, and it was not documented anywhere.

If you're going to install a switch on something, just remember to tell everyone involved, or it can cost a lot of time and effort chasing around nonexistent problems....

Elliott

🔥 Re: Hacking Web/FTP Servers (Cargill, [RISKS-20.21](#))

Andy Goldstein - VMS Development <goldstein@star.zko.dec.com>
Tue, 16 Feb 1999 22:45:49 -0500 (EST)

> write-protectable hard drives.

A quick perusal of the engineering specifications of the RZ-28 family (a 2GB 3.5" SCSI disk sold in recent years by Digital, now Compaq) shows a write-protect jumper. Bringing this out to a switch would be trivial. Most RZ-28 models were actually manufactured by Seagate. I can't speak for currently available models.

> Can anyone explain to me why such a scheme would be impractical or unworkable?

A certain popular server operating system does not support read-only volumes in its native file structure. Beyond that, the primary obstacle would appear to be lack of market demand.

[Followup: I looked at Seagate and Quantum's web sites, and the product descriptions for the high end disk drives show write protect jumpers for current models. AG]

⚡ Re: Hacking Web/FTP Servers (Cargill, [RISKS-20.21](#))

Rob Slade <rslade@sprint.ca>
Mon, 15 Feb 1999 15:40:21 -0800

HD write protection

> ... solution; write-protectable hard drives.

Great idea: simple, cheap, effective.

> Surely it would be very easy for HD manufacturers to produce drives with a
> *physical* 'off' switch which made it impossible to write to a drive unless
> you had physical access to the server. You would prepare updates

Ten years ago, or a little longer, we were pushing for the same thing in regard to computer viral programs. I suspect that some of the discussion

can be found in the RISKS archives. (It was about the time that PGN made an uncharacteristic lapse and didn't catch a reference to a "write-only" hard drive by one poster--or the two followups that quoted it.)

> Can anyone explain to me why such a scheme would be impractical or
> unworkable?

It would cost about as much, and be as difficult to handle, as the ubiquitous drive operating light. A simple rewiring of the drive line (which you can do yourself, if you have the ribbon cable schematics) makes an effective write protect: to tell the computer that the drive is currently protected, in order to give an error, might be a little more complicated. But not much.

No, I am at a loss to explain it. I even mentioned the fact in reviewing Western Digital's "Immunizer" system in 1992: they had this hugely complicated, interferring, and ultimately ineffective antiviral system when we had been asking them for years to produce a drive with a fifty cent write protect switch. Of course, doing the simple, effective thing would not have helped them try to sell the 7855 controller chip ...

rslade@vcn.bc.ca rslade@sprint.ca robertslade@usa.net
pl@canada.com

Re: Hacking Web/FTP Servers

Nigel Rantor <wiggly@bogo.co.uk>

Mon, 15 Feb 1999 12:59:02 +0000 (GMT)

I'm sure that RISKS will be deluged with answers to this particular question but I live in a world where web servers are my main concern at the moment, and so here goes;

For a web/ftp site that has no dynamic content, does not change very often *and* the administrator has physical access to a hardware *then* read/write protection switch *may* be an answer.

Unfortunately, in the real world most if not all web sites (not personal home pages which are even more of a nightmare from an administration point of view and I will not speak more of) have some form of dynamic content, and many of these do not use database backends, but store their data on the server's filesystem, either because they do not have access to a DB or they do not know how to use one.

Any well made website will also be updated frequently, websites suffer badly from bitrot like any information and a couple of weeks or a month can turn a cool site into yet another bookmark you will never see again.

Third strike coming up... How many web sites are hosted on virtual servers or co-located servers that have access to high bandwidth channels?

Most.

Our company doesn't want to invest in multiple T3's to be able to provide customers with class A bandwidth and support so we use a hosting company who provide high bandwidth, regular back ups and 24hr support with

on-site certified specialists. This does mean that we don't have physical access to the boxes though, and calling a support engineer to 'flip a switch' is, quite frankly, taking the piss.

Anyone who would support a physical system such as this because it is 'foolproof' is also deluding themselves, just because the data cannot be changed without physical access does not mean that other forms of attack will not be launched against a site. Denial of service attacks and rigged portals can be used to kill off a site's access or use the real site to gain information from the unsuspecting.

The final point I think must be this. If you think that you need a physical guard on your data then maybe you're not using the security tools that come with your system. Ensuring proper ACLs on resources is a huge step in the right direction. The number of sites that just let web servers write anywhere because it is more convenient for CGI writers is amazing. Proper guidelines for programmers about how the scripts must interact with the webserver are also a nice bonus, tell perl coders to use the -T flag, tell NT admins to install the most recent hotfixes for IIS to get rid of their DATA bugs. You don't even have to be paranoid, its basic good administration.

Nigel Rantor e-mail: wiggly AT bogo.co.uk / rantorn AT crowndigital.com

[Yes, we were deluged. I selected just three messages. PGN]

✂ Re: Computer fraud as another kind of Y2K risk? (Martin, [RISKS-20.21](#))

Chuck Karish <karish@well.com>

Sat, 13 Feb 1999 20:02:25 -0800

In [RISKS-20.21](#), Bruce Martin (Bruce_Martin@manulife.com) commented on the risk that an unscrupulous Y2K consultant might arrange to divert a client's funds during a period of uncertainty early next year.

The risk is broader than he suggests. Uncertainty whether systems are working properly will provide openings for many types of attacks, including social engineering as well as technical attacks: "We're fixing a critical problem that showed up when the clock struck midnight; would you relax security for a while so we can fix it?"

One sobering thought is that it may be weeks or months before the victims are certain that they can distinguish between theft and technical failure.

✂ Re: Computer fraud as another kind of Y2K risk? (Martin, [RISKS-20.21](#))

Dorothy Denning <denning@cs.georgetown.edu>

Mon, 15 Feb 1999 14:05:59 -0500

In [RISKS-20.21](#), Bruce Martin raised the possibility of a less-than-scrupulous Y2K consultant slipping in a few lines of

code in order
to "redirect a significant fraction of an organization's wealth
to a blind
account in the Cayman Islands at the stroke of midnight on 31
Dec 1999."

In June 1998, the *New York Post* ran a story about organized
crime setting
up a phony Y2K consulting firm for the purpose of diverting
money into
mob-controlled accounts. Adam Penenberg of Forbes Digital
investigated,
however, and found that the story had no substance. See
"Phantom Mobsters":
<http://www.forbes.com/tool/html/98/aug/0828/feat.htm>.

Dorothy Denning

✶ Re: Computer fraud as another kind of Y2K risk? (Martin, [RISKS 20.21](#))

Win Treese <treese@acm.org>
Mon, 15 Feb 1999 22:43:56 -0500

In [RISKS-20.21](#), Bruce Martin wonders about computer fraud
perpetrated
by miscreants among the legions of consultants working to fix
Y2K problems.

I've been wondering about a different kind of fraud, which
doesn't even require
expertise in computing. On January 1, 2000, withdraw \$1000 from
an ATM.
When you get the statement, complain to the bank that you didn't
make the
withdrawal. When they describe their records, repeat that you
never made
the withdrawal and ask "Do you have a Y2K problem here? Maybe I
should

call my attorney."

The problem for the bank, of course, is that proving that there wasn't a bug could be very costly--if not impossible.

Win Treese <treese@acm.org>

⚡ 8th USENIX Security Symposium: papers due March 9

Jennifer Radtke <jennifer@usenix.ORG>

Fri, 19 Feb 1999 01:04:32 GMT

August 23-26, 1999, Washington, D.C., USA

Sponsored by USENIX in cooperation with The CERT Coordination Center

If you are working in any practical aspects of security or applications

of cryptography, the program committee urges you to submit a paper.

REMINDER: Paper submissions due: 9 Mar 1999

Please find the Call for Papers at

<http://www.usenix.org/events/sec99/>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 23

Monday 1 March 1999

Contents

- [Intruders commandeer UK military satellite](#)
[PGN](#)
- [Software snafu slowed key data during Iraq raid](#)
[Paul Walczak](#)
- [Schwab Squab Swabbed](#)
[PGN](#)
- [Errant police computer wakes hundreds of Texans](#)
[Keith A Rhodes](#)
- [Mobile phones cause memory loss](#)
[Martin Minow](#)
- [Doctors to perform surgery over next-generation Internet](#)
[Keith A Rhodes](#)
- [Digital broadcasting could hit cardiac monitoring gear](#)
[Andrew Robert Mitchell](#)
- [Computer system results in errors in patient medical records](#)
[Doneel Edelson](#)
- [Pentium III serial number is soft-switchable after all](#)
[PGN](#)
- [Limiting liability for Y2K breakdowns](#)
[Edupage](#)

- [CIA predicts serious Y2K problems around the globe](#)
[Keith A Rhodes](#)
 - [Y2K Test Fine Test Data Causes Problem](#)
[Barry Frankel via Dave Farber](#)
 - [Self-inflicted single point of failure](#)
[Malcolm Pack](#)
 - [Rhode Islander sentenced for hacking](#)
[PGN](#)
 - [Profiling](#)
[Andrew Koenig](#)
 - [Re: Store Baelt Bridge not Y2K safe](#)
[Mark Brader](#)
[Chris Bagge](#)
 - [Computers, Freedom, and Privacy, 6-8 April 1999, Washington, DC](#)
[Dave Banisar](#)
 - [IEEE Security and Privacy Symposium, 9-12 May 1999](#)
[Jon Millen](#)
 - [USENIX Workshop on Smartcard Technology, 10-11 May 1999](#)
[Jennifer Radtke](#)
 - ['99 USENIX Technical Conference, 6-11 June, Monterey CA](#)
[Jennifer Radtke](#)
 - [FastAbstracts at FTCS29, 15-18 Jun 1999](#)
[Chuck Weinstock](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✚ Intruders commandeer UK military satellite

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

Mon, 1 Mar 99 8:42:12 PST

According to security sources cited by *The Sunday Business*, intruders have seized control of one of Britain's four military communication satellites -- over two weeks ago -- and demanded blackmail for them to stop interfering

with the satellite. [Source: Reuters item 28 Feb 1999, PGN-ed.
(*)]

[Several respondents remarked on this item, suggesting either that it was a hoax, or a very serious event that has been largely covered up. PGN]

[* For those of you who might ask, "PGN-ed" is a new verbal noun form (or, if you prefer, a nounal verb pun) implying that the item has been abstracted, summarized, or otherwise adapted for RISKS without violating any copyrights, that is, ``PGN-ed'', which is intended to be pronounced either as ``pee-gee-en'd'' or ``pee-gee-en-ed'', according to your verbal and nounal linguistic preferences, respectively.]

🔥 Software snafu slowed key data during Iraq raid

<Paul_Walczak@mail.arl.mil>
Fri, 26 Feb 1999 17:18:53 -0500

The U.S. Department of Defense is still studying the software glitch that caused DOD's \$184 million Global Transportation Network (GTN) to have up to eight-hour delays in the availability of updated worldwide logistics information during the December 1999 Desert Fox bombing operations, despite GTN having being designed to provide updates worldwide within 30 seconds. GTN has 23 interfaces with other systems. [Source: Article by Daniel Verton (dan_verton@fcw.com), Federal Computer Week, week of 22 Feb 1999.]
[Reference added in archive copy. PGN]

✈ Schwab Squab Swabbed

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

Mon, 1 Mar 99 15:12:06 PST

Charles Schwab & Co's electronic brokerage Website and Street Smart computer system were off the air for an hour and one-half, beginning 5 minutes after trading opened on the NYSE on 24 Feb 1999. The outage was the result of a software upgrade to hook in a new mainframe system in Phoenix, which failed to take flight. This follows failures of other on-line brokerage systems (E-Trade, Waterhouse, Ameritrade, and Datek) in recent weeks. I guess the market pressures are too great for anyone to take the time to do it right. [Source: *San Francisco Chronicle*, 25 Feb 1999, B1. PGN-ed. However, the fledgling Phoenix system eventually rose from its ashes. Pigeon pennies, anyone?]

✈ Errant police computer wakes hundreds of Texans

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

Fri, 26 Feb 1999 08:16:39 -0500

A police computer in Fort Worth TX made 1,300 phone calls to invite residents to a police community forum -- beginning at 3 a.m. Sunday morning, instead of during the day. [Source: Reuters item 25 Feb 1999,

PGN-ed. At
least 400 people answered, and heard the programmed caller
identified as
"reverse 911" -- which sounds like "YOU ARE IN TROUBLE" rather
than "I AM IN
TROUBLE".)

⚡ Mobile phones cause memory loss

Martin Minow <minow@apple.com>
Mon, 1 Mar 1999 16:20:38 -0800

<<http://www.theregister.co.uk/990301-000021.html>>

Today's [London] *Daily Mail* reports that mobile phones cause
memory loss.
This link was demonstrated by a hospital in Bristol, which
attached
transmitters to the heads of volunteers, some with microwaves,
others with
none. On subsequent tests of mental acuity, the radiated
patients did
significantly worse than the rest. [Presumably relative to
their previous
behavior. The report is rather vague. PGN-ed]

⚡ Doctors to perform surgery over next-generation Internet

"Keith A Rhodes" <rhodesk.aimd@gao.gov>
Wed, 24 Feb 1999 11:08:44 -0500

The \$500M Abilene Network is planned as a 2.4 gigabit/sec link
among a few
dozen research universities. To demonstrate this, a doctor in
Washington
DC's Union Station will work with a surgical team at Ohio State

performing
laparoscopic surgery on a volunteer patient suffering from a
gastrointestinal disorder [an Internaut? seeking gut
reactions?]. [Source:
Article by Ted Bridis, Associated Press, 23 Feb 1999, PGN
Abstracting]

[Plans for live surgery rather than just remote advice are in
the offing.
<Pun NOT INTENDED.> Hopefully, by then the reliability,
security, and
general availability of networked systems will have improved
sufficiently
that would avoid risks of computer and network outages during
open-brain
surgery. PGN] (Stephen Wolff of Cisco Systems Inc. was quoted
as asking one
of the RISKS-related questions that comes to mind: "Can a
surgery and
multiplayer Doom coexist on a network?" [Cisco supplied about
\$5 million
worth of high-tech network equipment for Abilene.]

[NOTE: They never discuss the stability of the network, do they?
Why does
this article remind me of the Star Trek episode where Dr. McCoy
is rewiring
Mr. Spock's brain? About half-way through the surgery -- which
McCoy had
described as "child's play" just prior to the commercial break
-- McCoy
starts to realize that he doesn't know what he's doing because
the helmet
he's wearing with all the knowledge in it is starting to fail?
Anyone should
be able to figure out when to launch the denial-of-service
attack against
the remote connection. Aren't there plenty of critical moments
in just
routine surgery? In this case, there's a world-class specialist
helping out
a not-so-world-class specialist, because the surgery is
important for some

reason. A bunch of untraceable broken packets have no place in delicate vascular surgery. KAR]

[Archive copy corrected to Abilene. PGN]

⚡ Digital broadcasting could hit cardiac monitoring gear

Andrew Robert Mitchell <andrewm@cse.unsw.edu.au>

Fri, 26 Feb 1999 20:54:42 +1100

[Source: ABC News Australia,

<http://www.abc.net.au/news/state/vic/metvic-26feb1999-15.html>]

> Cardiac monitoring equipment in a number of Australian hospitals is at
> risk of malfunctioning due to digital broadcasting interference.
> Melbourne's Epworth Hospital claims heart patients were put at risk
> recently because a television station was given the same digital channel
> it uses to monitor heart patients. The hospital was unaware Channel Seven
> had been sold a licence to use part of the spectrum for tests ahead of
> digital broadcasting.

The risk is obvious: <insert name of boring show> causes panic at hospitals as all cardiac monitoring equipment falsely measures zero ;)

Andrew Mitchell <andrewm@cse.unsw.edu.au>

[Also noted by Iain "Kaos" Holmes <kaos@cabernet.ctrl.com.au>. PGN]

⚡ Computer system results in errors in patient medical records

"Edelson, Doneel" <doneeledelson@aciins.com>

Fri, 26 Feb 1999 12:26:31 -0500

Vancouver Hospital installed a new computer system in mid 1997 that sends pathology reports on-line to the attending physicians. However, the software did not automatically update the patients' charts (unless staff members used a special code, which apparently they usually did not), significantly delaying treatments and discharges, and increasing costs.

[From Leonard Lee's Glitches of the week, Newsbytes News Network <<http://www.newsbytes.com/>>, 24 Feb 1999, PGN-ed]

["Leonard Lee is a nationally recognized consultant and frequent speaker on computer errors. Readers are encouraged to e-mail news clippings of interesting computer glitches at www.homestead.com/doctorglitch <<http://www.homestead.com/doctorglitch>>."]

⚡ Pentium III serial number is soft-switchable after all

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

Mon, 1 Mar 99 15:17:47 PST

After all the fuss about the risks of the Pentium III unique serial number, and Intel's claim that it can be permanently masked, a report from the German C't News says that despite Intel's claims, the ability to read the serial number can be turned on and off remotely under software control, without the user's knowledge. The trick uses only documented

features.

[Source: Christian Persson, *Computer Technology*, c't news, translated by

Juergen Kuri, dated 24 Feb 1999, also noted by Leander Kahney in Wired News,

23 Feb 1999 [note the time difference; c't article preceded Wired],

<http://www.wired.com/news/news/technology/story/18078.html> . PGN

⚡ Limiting liability for Y2K breakdowns

Edupage Editors <edupage@franklin.oit.unc.edu>

Thu, 25 Feb 1999 13:35:16 -0500 (EST)

A bipartisan group in the U.S. House of Representatives has introduced

legislation that would limit litigation, lawyers' fees, and damages caused

by Y2K-related computer breakdowns. Supporters of the bill claim that it

would help avert Year 2000 problems, since the legislation would protect

only those businesses and individuals who take reasonable actions to prevent

them from occurring. (*The New York Times*, 24 Feb 1999, Edupage, 25

February 1999) [CA, FL, GA, HA, NV, and VA have already passed such laws.

31 other states are considering such legislation. There are of course also

risks of this making the situation worse as well. PGN]

⚡ CIA predicts serious Y2K problems around the globe

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

Thu, 25 Feb 1999 09:12:16 -0500

Amidst all the discussion of possible Y2K effects is the issue of foreign government preparedness. Air Force Gen. John Gordon, deputy director of the CIA, appeared at a hearing of the Senate Armed Services Committee and testified that other countries (including Russia) are far behind in preparing for possible crises, noting in particular breakdowns in nuclear reactors and strategic missile systems, midwinter power outages and disruptions in world trade and oil shipments. However, he discounted the possibility of accidentally missile launches due to Y2K. But he did add that malfunctions in temperature and humidity monitors could lead to incorrect information. He said that China will probably experience failures in key sectors such as telecommunications, electric power and banking.
[Source: AP item by Jim Abrams, 25 Feb 1999, PGN Abstracting]

✦ Y2K Test Fine Test Data Causes Problem (via Dave Farber)

Barry Frankel <bfrankel@ix.netcom.com>
Sat, 27 Feb 1999 09:19:42 -0500

Last October, PSE&G sent incorrect bills to 61,000 of their customers as a result of an operator error. Subsequent to testing their billing system for Y2K compliance, the residues from the test data were not properly removed, resulting in erroneous statements of past payments and amount owed. However, this error was announced only recently. [Source: New Jersey

Online, *The Times* (Mercer County, NJ); this item has been PGN-
ed from

<http://www.nj.com/mercerc/times/stories/02-27-Q2BBFUMB.html> .]

✶ Self-inflicted single point of failure

Malcolm Pack <m.pack@cableinet.co.uk>

Mon, 22 Feb 1999 06:51:30 GMT

At approximately 04:10 on Sunday 21 Feb 1999, a transatlantic communications link belonging to Teleglobe developed a fault. By 19:30 that evening the fault (whatever it was) was repaired. In the interim period, almost all Internet connectivity, both within and outside the UK, was lost to customers of Teleglobe, of one of its major partners (and my main ISP) Cable Internet, and other ISPs taking their feeds from these two companies, including many of the UK's new "free" services such as Telinco and Aardvaak.

The situation was compounded by a mail server upgrade which Cable Internet started at 4am, as part of which *all* routes and DNS caching were reset. With no easy path to other countries, routers failed to discover new routes and DNS lookups failed consistently.

I have access to another free ISP apparently unaffected by the cable outage; but found it too slow to be of any use. That this was caused by increased traffic as new routes were found, and increased logging-in by users abandoning their primary ISPs, is mere speculation; but my son had to do

without a better translation than the one I could offer of a key passage in "Le Roman de la Rose" because of timeouts on many search engines and their results.

All this is normal fare for the Internet. It is a non-guaranteed service, after all. That there were no backup routes in place even 12 hours after the failure is annoying, but I await an explanation of this from Cable Internet.

I was more bemused by the number of people posting messages on Cable Internet's support newsgroup complaining that they were unable to run their Internet-reliant businesses because of Cable Internet's failure to provide a backup service. Naturally, not one of them had made his or her own provision for a backup by using another ISP.

What this all says about single points of failure is self-evident.

Malcolm Pack <m.pack@cableinet.co.uk>



⚡ Rhode Islander sentenced for hacking

"Peter G. Neumann" <neumann@csl.sri.com>
Tue, 23 Feb 99 18:14:24 EST

Sean Trifero was sentenced to one year in prison by a U.S. District Judge for intentionally damaging computer systems (Harvard, Amherst, a Florida ISP, and Alliant Technologies, including planting sniffers and denial-of-service attacks) and unauthorizedly accessing others (Arctic

Slope Regional

Corp. and Barrows Cable, Alaska), three years subsequent probation, 150

hours of community service, and \$31,650 restitution. [Source: PRNewswire, 23 Feb 1999]

Profiling

Andrew Koenig <ark@research.att.com>

Fri, 26 Feb 1999 11:08:01 -0500 (EST)

Recently, my wife and I ordered a bunch of tableware from a local jewelry-and-china-and-crystal store. Because of our slightly unusual taste,

we had the honor of being the first customers ever to order some of those

items, which meant that the store had no entries in their database for them.

They therefore separated our order into two orders, one for the items that

their database knew about, and the other for the new ones.

Because there

were two orders, there were two charge tickets.

Four days later, after we had finished dinner in a restaurant, and half an

hour before curtain time for the play we were about to see, our waiter

informed us that he had put our credit card through the machine twice, that

it had been declined twice, and that he could call them and talk to them if

we liked. The ensuing confusion, which took long enough to clear up that we

came within eight minutes of missing our play, involved not only our waiter

but the restaurant manager, who said that the credit card people had

eventually approved the purchase, but that we were to call them at our earliest convenience.

The problem, of course, was that two purchases in rapid succession at a jewelry store had tripped the credit card company's fraud detectors, so they wanted to be sure that we were still in possession of the card and that we had actually made those purchases. They had been meaning to call us, but hadn't gotten around to it yet.

The risk? Expert-system profilers are adding all kinds of unwritten rules to our lives, with various kinds of inconvenience and harassment as the penalty for violating them.

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

✉ Re: Store Baelte Bridge not Y2K safe (Weber-Wulff, [Risks-20.22](#))

Mark Brader <msbrader@interlog.com>
Sun, 28 Feb 1999 22:48:55 -0500 (EST)

Not quite right. The west half of the Storebaelte crossing consists of a side-by-side road and rail bridge, but the east half has a separate road bridge while the railway uses a tunnel. It's the east bridge that opened last year; the railway (which is presumably the part with a Y2K problem) opened in April 1997 to freight and June 1997 to passenger trains.

See <<http://www.railway-technology.com/projects/denmark/>> for a description of the crossing in English. (However, it never had the world's longest main span, as claimed; the Akashi-Kaikyo Bridge in Japan is longer and opened a month or two earlier.)

Mark Brader, Toronto, msbrader@interlog.com

✂ Re: Store Baelte Bridge not Y2K-safe (Weber-Wulff, [RISKS-20.22](#))

Chris Bagge <CBB@delta.dk>

Mon, 22 Feb 1999 11:14:14 +0100

The problem is mainly not with the bridge, but with the double train-tunnel running in parallel. This tunnel was heavily delayed during construction, due to 'the-fault-that-cannot occur', as both tunnel were flooded!

The only limit on the road bridge would be the toll-gates, and there is a fast (and cheap :-)) solution to that problem.

Regards

Chris Bagge

✂ Computers, Freedom, and Privacy, 6-8 April 1999, Washington, DC

Dave Banisar <banisar@epic.org>

Sat, 20 Feb 1999 15:01:54 -0500

Register now for the cyber event of the year (cfp99.org)

COMPUTERS, FREEDOM, AND PRIVACY:
THE GLOBAL INTERNET

WASHINGTON, DC
Omni Shoreham Hotel
April 6-8, 1999

For almost a decade, the conference on Computers, Freedom and Privacy has shaped the public debate on the future of privacy and freedom in the online world. Register now for the number one Internet policy conference. Join a diverse audience from government, industry, academics, the non-profit sector, the hacker community and the media. Enjoy the U.S. Capital in the Spring at one of Washington's premier hotels.

* Keynote speakers include Tim Berners-Lee (Director, World Wide Web

Consortium), Vint Cerf (President, Internet Society),
Congressman Ed

Markey (sponsor of "The Electronic Bill of Rights Act"),
Congressman Ron

Paul (sponsor of the Freedom and Privacy Restoration Act),
Henrikas

Yushkiavitshus (Associate Director, UNESCO)

* Lively and thought-provoking panels on -- "the Creation of a Global

Surveillance Network," "Access and Equity on the Global Internet,"

"Anonymity and Identity in Cyberspace," "Free Speech and Cyber Censorship," "Is Escrow Dead? And what is Wassenaar?", "Self-Regulation

Reconsidered" and more

* Tutorials -- "The Electronic Communications Privacy Act" (Mark Eckenwiler); "Cryptography: Basic Overview & Nontraditional Uses" (Matt

Blaze and Phil Zimmermann), "Free Speech, The Constitution and Privacy in Cyberspace" (Mike Godwin), "Techniques for Circumventing Internet Censorship" (Bennett Haselton and Brian Ristuccia)

Early Registration Deadline - March 15, 1999

Register on-line at <http://www.regmaster.com/cfp99.html> or call +1 407 628 3602. Registration inquiries may also be sent to mann@regmaster.com.

For more information about CFP99, visit <http://www.cfp99.org/> or call +1 401 628 3186

Sponsored by the Association for Computing Machinery

David Banisar (Banisar@epic.org), Electronic Privacy Information Center,
666 Pennsylvania Ave, SE, Suite 301 Washington, DC 20003 <http://www.epic.org>

IEEE Security and Privacy Symposium, 9-12 May 1999

Jon Millen <millen@csl.sri.com>
Mon, 01 Mar 1999 09:54:36 -0800

1999 IEEE Symposium on Security and Privacy
Special 20th Anniversary Program

9-12 May 1999

The Claremont Resort
Berkeley, California

Sponsored by the IEEE Technical Committee on Security and Privacy

In cooperation with the International Association of Cryptologic Research

Symposium Committee:
John McLean, General Chair

Jonathan Millen, Vice Chair
Li Gong, Program Co-Chair
Michael Reiter, Program Co-Chair

Advance registration deadline 5 Apr 1999.

Abridged for RISKS. Full registration info:

<http://www.csl.sri.com/~millen/sp99prog.txt>

PRELIMINARY PROGRAM

Monday, May 10, 1999

8:45am-9:00am Welcome: Chairs

9:00am-10:30am Systems, Session Chair: Roger Needham, Microsoft Research

Hardening COTS software with generic software wrappers

Timothy Fraser, Lee Badger, Mark Feldman

TIS Labs at Network Associates, Inc.

Firmato: A novel firewall management toolkit

Yair Bartal, Alain Mayer, Kobbi Nissim, Avishai Wool, Lucent Bell Labs

Flexible policy-directed code safety, David Evans, Andrew Twyman, MIT

11:00am-12:00pm Policy, Session Chair: Ravi Sandhu, George Mason University

Local reconfiguration policies

Jonathan K. Millen, SRI International

A modular, user-centered authorization service built on an RBAC foundation

Mary Ellen Zurko, Richard T. Simon, Tom Sanfilippo, Iris Associates

12:00pm-12:30pm Surprise

2:00pm-3:00pm Verification, Session Chair: John Mitchell, Stanford University

Secure communications processing for distributed languages

Martin Abadi, Cedric Fournet, Georges Gonthier

Compaq Systems Research Center, Microsoft Research, and INRIA

Verification of control flow based security policies

T. Jensen, D. Le Metayer, T. Thorn
IRISA

3:30pm-5:00pm Panel Discussion

Brief History of Twenty Years of Computer Security Research

Panel Chair: Teresa Lunt, Xerox PARC

Panelists:

G.R. Blakley, Texas A&M University

20 years of cryptography

Virgil Gligor, U Maryland

20 years of operating system security (Unix as one
focus)

Steve Lipner, MITRETEK

20 years of criteria development/commercial technology

Jonathan K. Millen, SRI International

20 years of covert channel modeling and analysis

John McLean, NRL

20 years of formal methods

Steve Kent BBN/GTE

20 years of network security

Tuesday, May 11, 1999

9:00am-10:30am Intrusion Detection

Session Chair: Cynthia Irvine, Naval Postgraduate School

A data mining framework for building intrusion detection models

Wenke Lee, Sal Stolfo, Kui Mok, Columbia University

Detecting intrusions using system calls: Alternative data models

Christina Warrender, Stephanie Forrest, Barak Pearlmutter
University of New Mexico

Detecting computer and network misuse through the production-
based

expert system toolset (P-BEST)

Ulf Lindqvist, Phillip A. Porras, SRI International

11:00am-12:30pm Panel 2

Near Misses and Hidden Treasures in Early Computer Security

Research

Panel Chair: Stan Ames, MITRE

Panelists: Tom Berson, Anagram Labs and Xerox PARC

Marv Schaefer, Arca

Dick Kemmerer, UC Santa Barbara

2:00pm-3:30pm Information Flow

Session Chair: John McHugh, Portland State University

A multi-threading architecture for multilevel secure transaction processing

Haruna Isa, William R. Shockley, Cynthia E. Irvine

U.S. Navy, Cyberscape Computer Services, and Naval Postgraduate School

Specification and enforcement of classification and inference constraints

Steven Dawson, Sabrina De Capitani di Vimercati, Pierangela Samarati

SRI International and University of Milan

A test for non-disclosure in security level translations

David Rosenthal, Francis Fung

Odyssey Research Associates

4:00-5:30pm Work-In-Progress (5-minute Presentations)

Session Chair: Heather Hinton, Ryerson Polytechnic University

Wednesday, May 12, 1999

9:00am-10:00am Authentication and Key Exchange

Session Chair: Dieter Gollmann, Microsoft Research

Software smart cards via cryptographic camouflage

D. Hoover, B. N. Kausik, Arcot Systems

Analysis of the internet key exchange protocol using the NRL protocol analyzer

Catherine Meadows, Naval Research Laboratory

10:30am-12:00pm. Panel Discussion

Time Capsule -- Twenty Years From Now

Panel Chair: Michael Reiter, Lucent Bell Labs

Panelists:

Mark Weiser, Xerox PARC, Future of computing

Roger Needham, Microsoft Research, Cambridge
Future of hardware technology

Howard Shrobe, MIT AI Lab, Future of software technology

Hilarie Orman, DARPA, Future of networking

Brian Snow, National Security Agency, Future of Security

⚡ USENIX Workshop on Smartcard Technology, 10-11 May 1999

Jennifer Radtke <jennifer@usenix.ORG>

Sat, 27 Feb 1999 00:14:52 GMT

10-11 May 1999, McCormick Place South, Chicago, Illinois, USA

For Researchers, Product Developers and Smart Card Deployers

Review the full program and register online at

<http://www.usenix.org/events/smartcard99/>

Save when registering before Friday, April 16, 1999

⚡ '99 USENIX Technical Conference, 6-11 June, Monterey CA

Jennifer Radtke <jennifer@usenix.ORG>

Mon, 1 Mar 1999 23:40:46 GMT

A conference by and for programmers, developers, and system administrators working in advanced systems and software.

1999 USENIX ANNUAL TECHNICAL CONFERENCE

June 6-11, 1999, Monterey, California

<http://www.usenix.org/events/usenix99>

TUTORIALS, 23 REFEREED PAPERS,

FREENIX TRACK--Quality Technical Forum Devoted To Open Source Software.

John Ousterhout, creator of Tcl/Tk, will focus his keynote on a fundamental shift in software development to integration applications.

✦ FastAbstracts at FTCS29, 15-18 Jun 1999

Chuck Weinstock <weinstock@sei.cmu.edu>

Tue, 23 Feb 1999 16:52:11 -0500

The Fault-Tolerant Computing Symposium is being held in Madison Wisconsin, 15-18 Jun 1999.

Continuing a new tradition at FTCS, we are pleased to announce the FastAbstracts session. FastAbstracts are intended as a mechanism to:

- report on current work that may or may not be complete
- introduce new ideas to the community
- state positions on controversial issues ("Outrageous Opinions")

Participants in this session will present a short talk (5 to 8 minutes including 1 minute for questions), and publish a concise and succinct (two pages) abstract in a printed proceedings. A web version of the abstract will also be available on the FTCS website.

Full details regarding FTCS and the FastAbstracts submission process are available at <<http://www.ftcs.org>>.

Chuck Weinstock, FastAbstracts Chair, FTCS-29



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 24

Thursday 11 March 1999

Contents

- [Risks of testing a nuclear power plant for Y2K compliance](#)
[Robert Brill](#)
- [ATC Equipment test almost causes landing collision in Australia](#)
[Pat Dirks](#)
- [win9x instability?](#)
[Norman Choe](#)
- [Outlook Express Date: parsing](#)
[Kenneth C. Dyke](#)
- [Fonte des neiges](#)
[Bertrand Meyer](#)
- [Risks of voice-recognition software](#)
[Chris Leeson](#)
- [Rogue spelling checker at work](#)
[Andrew Koenig](#)
- [Glitch opens jail cell doors](#)
[David Kennedy](#)
- [Super Hornet](#)
[PGN](#)
- [Italian hospitalized for hallucinations after Net surfing spree](#)
[Lloyd Wood](#)

- [Damning critique of WIPO Internet domain name proposal](#)
[Lance J. Hoffman](#)
 - [Bringing Y2K fears to a new high -- or low](#)
[Michael P. Gerlek](#)
 - [Regular break-ins at the Pentagon?](#)
[Martin Ward](#)
 - [Re: Remote surgery](#)
[Declan O'Kane](#)
 - [More on-line trauma](#)
[JJSantos](#)
 - [Re: Lack of Anonymity in Microsoft Word](#)
[Yvo Desmedt](#)
 - [Re: Write-protectable hard-drives](#)
[Richard Schroepel](#)
 - [Networking'99--NetAdmins & SysAdmins Share Solutions](#)
[enotify](#)
 - [Workshop on Countering Cyber-Terrorism](#)
[Clifford Neuman](#)
 - [PDPTA'99 on Fault Tolerance and Reconfiguration in Distributed Systems](#)
[Pradip Srimani](#)
 - [FMICS4](#)
[Diego Latella](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Risks of testing a nuclear power plant for Y2K compliance

Robert Brill <RWB2@nrc.gov>
Mon, 08 Mar 1999 16:20:22 -0500

Pennsylvania's Peach Bottom Atomic Power Station was subjected to detailed software analyses and simulations to check Y2K compliance, and concluded that everything would be OK. However, when the clock was moved ahead, the primary and backup monitoring systems crashed, every computer

screen blanked out, and forced manual procedures. The cause was attributed to a technician improperly setting the test clock. The systems remained down for seven hours. ``Although the cause was human error, technology specialists say the glitch here illustrates an unanticipated peril of the Year 2000 problem: As computer systems that have been repaired are now being tested in live conditions, inadvertent mistakes and undiscovered bugs can bring the machines -- and the organizations that rely on them -- to a grinding halt.''
[Source: Rajiv Chandrasekaran, Big Glitch at Nuclear Plant Shows Perils of Y2K Tests, *The Washington Post* A03, 7 Mar 1999. PGN-ed]

✈ ATC Equipment test almost causes landing collision in Australia

Pat Dirks <pwd@apple.com>
Mon, 8 Mar 1999 14:51:55 -0800

I snipped this item (A Pull-Up Down-Under) from AvWeb's AVflash. It's a weekly mailing of aviation-related items from AvWeb (www.avweb.com):

Controllers in Sydney, Australia last week during a temporary communications outage (due to testing of new equipment) could only watch as a Boeing 747-400 with 220 passengers on final approach headed for a 36-seat Dash 8 on the runway. Fortunately, the 747 pilot (whose final clearance had not been received due to the outage) pulled up at the last moment,

missing the Dash
by 200 feet. [Full story at <http://www.avweb.com/newswire/news9910.html#7>;
PGN-ed]

Note from PWD: ordinary, internationally accepted rules prohibit landing without an explicit clearance. The Boeing 747 should not have landed but, of course, it's only too easy to assume that, having gotten this far without a word from the tower to the contrary, landing clearance had been granted.

In the event of communications failure (or to communicate with planes not equipped with a radio) light signals are used from the control tower: a red light is a signal NOT to land, so the tower reacted appropriately to the situation. A 747 pilot whose radios are in fine working order won't be LOOKING for light signals from the tower, of course.

This does, indeed, sound like a close call and highlights the dangers of working on or around complex systems that are in active use.

win9x instability?

Norman Choe <norman@environs.com>
Thu, 4 Mar 1999 16:28:30 -0500

Computer Hangs After 49.7 Days

The information in this article applies to:

Microsoft Windows 95
Microsoft Windows 95 OEM Service Release versions 2, 2.1,

2.5

Microsoft Windows 98

SYMPTOMS

After 49.7 days of continuous operation, your Windows 95-based computer may stop responding (hang).

CAUSE

There is a problem with the timing algorithm in the Vtdapi.vxd file.

(taken from <http://support.microsoft.com/support/kb/articles/q216/6/41.asp>)

However, i would like to point out that Microsoft already has a good fix for this... there's no way in hell any win 9x machine could possibly run for that long without crashing ANYway, so this instability is purely theoretical.

norman@environs.com <http://www.environs.com/>

[Intriguingly, there may be some evidence to the contrary! In December 1998, Ed Felten's testimony for the Justice Department indicated that during the previous seven months he had been running Windows 98 more or less uninterruptedly at Princeton, *after* removing Internet Explorer (using the program that he demonstrated to DoJ). He testified that there had been no unexplained crashes during that period. Meanwhile, many other folks report that various windows versions typically require a reboot as often as every week or two. Incidentally, the actual "hang-time" is roughly 49.710269 days, which corresponds to

2^32 milliseconds. This was noted by several correspondents, including

Andrew Koenig <ark@research.att.com>, who asks,

``Isn't a 32-bit millisecond counter even sillier than a 2-digit year counter?''

Ah, yes. I don't think I have mentioned Multics' 1965 choice of a 71-bit

microsecond clock recently enough, so let me do it again. A little bit

of foresight (well, actually, quite a few bits) deserves some Y2Kudos.

PGN]

✶ Outlook Express Date: parsing

"Kenneth C. Dyke" <kcd@jumpgate.com>

Sat, 6 Mar 99 00:12:23 -0800

Given that I typically sort my inbox based on Date Sent, with newer e-mail at the top, it seemed odd to see messages showing up at the top of my list with dates such as this:

Fri, Aug 1, 1919, 12:28 PM

Being curious, I took a look at the actual Date: line in the header:

Date: Sun, 4 Jan 2099 18:28:02 -0200

So, one obviously bogus date is somehow parsed to be in the future (according to how it was sorted in the list), but is then displayed as being 80 years old.

Sadly, this wasn't the only case I found. I also had a piece of e-mail with the following date header:

Date: 6/30/98 11:14:34 PM Pacific Daylight Time

Outlook Express displayed it as:

Mon, Jul 30, 2018, 3:14 AM

Interestingly, it displayed it **above** most of my other mail (which is dated correctly from 1999), but **below** the bogus mail shown up above.

I suddenly have renewed faith in Microsoft's Y2K efforts.

-Ken

✶ Fonte des neiges

<Bertrand.Meyer@eiffel.com>
Sat, 6 Mar 1999 11:39:48 -0800

Here is a new, although perhaps unconscious, addition to the growing practice of applying computer terminology to other walks (or in this case runs) of life, as in "the economy needs rebooting".

If you go skiing at Mountain High in San Bernardino county, California, you will see at the top of the main lift in the West Resort a sign stating various regulations, ending (I swear I am not making this up) with the following injunction in upper case:

NO INVERTED ARIAL

As someone who frequently needs Unix fonts to match Windows ones, I knew exactly what the rule would have been if this had been Zermatt:

NO INVERTED
HELVETICA.

The possibilities for more such rules, in the PGN* style, appear almost endless. I don't know if it was a result of the eth-Arial atmosphere up there, but when running down the slopes I could think of quite a few, a couple of which I am including here for fear of being PGNed**:

- On the way down, don't be too Bold!
- NEVER fall on your TypeFace. The Impact might make you look Comic (especially if it leaves you Sans your skis).

These are all Modern but, ever the Bookman, I had a few more literate ones, from some older Century Schoolbook, such as:

- When in Rome, ignore the rest of Italics: do as the Roman does.

(Although at Times you should do as the New Roman.)

I hope this (delivered by Courier to the comp.risks Bookshelf) is a welcome diversion from the usually more Aerial topics of comp.risks.

Oh, and for anyone who missed the profoundly subtle cross-linguistic Subject header: Fonte is a translation of the English word "font" into French computerese (replacing the proper French term), but also means, among other things, melting, so that "fonte des neiges" is melting of the snows (thaw) as well as font of the snows.

I still fear that the Moderator will have a few additions of his own, at least if he remains True to Type -- or is this just TrueType?.

* Puns Grossly Noxious

** Preempted Gracefully by Neumann

-- Bertrand Meyer

Interactive Software Engineering, Santa Barbara, <Bertrand.Meyer@eiffel.com>

Melting *Ice* expert, see <http://eiffel.com/products/bench/>

[I'm thawed of as very font of contributions such as Bertand's.
'Snow joke. (Are we playing Al-fonts and Gaston with E-le-fonts?)

Merci! Pierre/PGN]

⚡ Risks of voice-recognition software

"LEESON, Chris" <CHRIS.LEESON@sema.co.uk>

Thu, 11 Mar 1999 10:52:13 -0000

Quoted from an article appearing in the "Backbytes" section of Computing (11 March 1999); The article describes a demonstration of some voice-recognition software:

> A representative from the company was just about to start the
> demonstration and asked everyone in the room to be quiet.

> Just then someone in the back of the room yelled: 'Format c:
Return".

> Someone else chimed in: "Yes, Return"

> Unfortunately the software worked!

I seem to remember someone in an earlier RISKS posting suggesting a similar scenario using words (maliciously) planted into a music CD ("Delete my files"/"Yes, I'm sure"). Unfortunately I cannot find the original posting.

[[RISKS-19.25](#) and [20.10](#) were recent item on this topic, although it has certainly been an ongoing theme... PGN]

✶ Rogue spelling checker at work

Andrew Koenig <ark@research.att.com>
Sun, 7 Mar 1999 13:01:31 -0500 (EST)

Headline from AP wire today: ``Pope Beautifies 10 more''

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

[Papal ben-E-diction? Vaticanonesses? Vaticanan ladies? PGN]

✶ Glitch opens jail cell doors

David Kennedy CISSP <dmkennedy@compuserve.com>
Wed, 03 Mar 1999 23:50:20 -0500

RISKS has reported numerous cases of prison doors opening or not opening because of computer malfunctions. In the latest episode, cell doors on the ninth floor of the Kenton County Detention Center in Covington KY opened spuriously and remained open for 9.5 hours, although the convicts were still confined within a larger area. [Source: The Cincinnati Enquirer, 3 Mar 1999, http://enquirer.com/editions/1999/03/03/loc_glitch_opens_cell.html]; PGN-ed. Good case for layered security, domains of protection,

etc.]

David Kennedy CISSP Director of Research Services ICSA Inc.
<http://www.icsa.net>

✶ Super Hornet

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

Wed, 10 Mar 99 10:50:53 PST

Defense Daily (vol 201, no 43, page 1) reports that in a Senate hearing Senator Chuck Robb (D-Virginia) raised the issue of obtaining an unclassified version of a report on the Navy's Operational Test IIB of the F/A-18E/F Super Hornet aircraft. [In the absence of information (the Navy has denied a FOIA request), it is not clear who may be getting stung by the Hornet's performance (or lack thereof?). PGN-ed]

✶ Italian hospitalized for hallucinations after Net surfing spree

Lloyd Wood <L.Wood@surrey.ac.uk>

Wed, 3 Mar 1999 13:22:14 +0000 (GMT)

An Italian man was diagnosed with 'acute Internet intoxication' (including delirium and mental confusion) attributed to his spending three straight days surfing the Internet. A psychiatrist in Rome suggested that this was not unusual, believing that several hundred Romans were suffering as well. He claimed most of those were around 30, single, educated, and with no prior

history of mental problems, all spending at least 10 hours a day on-line, and he recommended keeping use under 5 to 6 hours a day. That would seem to put a lot of us at risk.

[Lloyd forwarded a message to me from glen mccready <glen@qnx.com>

to 0xdeadbeef@substance.blackdown.org with the above Subject, reforwarding a copyrighted article from nandotimes.com, 2 Mar 1999, that

came via William Knowles <erehwon@kizmiaz.dis.org>. As we approach April

Fool's Day, it seems to be more difficult to separate the wheat from

the chaff, as in the case of "Mobile phones cause memory loss" in

[RISKS-20.23](#), which is speculative at best. I have adapted the nandotimes

item for RISKS, although it falls in a similar category. PGN-ed]

🔥 Damning critique of WIPO Internet domain name proposal

"Lance J. Hoffman" <hoffman@SEAS.GWU.EDU>

Sun, 07 Mar 1999 23:32:22 -0500

Just in time for the last public hearing this coming Wednesday (10 Mar 1999)

in Washington, law professor Michael Fromkin of the University of Miami has

issued on his web page a damning critique of the current domain name

proposal of the World Intellectual Property Organization. I'll let his

paper speak for itself, but this issue is so important to the future of an

Internet-enhanced society that I urge wide circulation and reading of the

Froomkin critique before a grand disaster is set up by an organization with tenuous legitimacy and experience in Internet-related matters, but with plenty of baggage from the existing powers-that-be. I've reproduced just the opening part below, but URLs to more detailed arguments are given there.

From Froomkin's Web page (<http://www.law.miami.edu/~amf/quickguide.htm>):

Major Flaws in the WIPO Domain Name Proposal -- A Quick Guide
A. Michael Froomkin, Professor of Law

Executive Summary

The World Intellectual Property Organization's plan to restructure the way Internet domain names in .com, .net, and .org are assigned and adjudicated is deeply flawed. The plan, contained in WIPO's "Interim Report" is designed to solve problems caused when Internet domain names collide with trademarked words. WIPO was asked to make suggestions for better dispute resolution, and it claims to have produced a plan that creates no new rights for intellectual property holders. In fact, however, the plan would impose extensive Alternate Dispute Resolution on all domain name registrants accused of infringing of any type of intellectual property with their registration.

The WIPO plan's flaws include:

- * Bias. The plan is biased in favor of trademark holders
- * Enabling censorship. The WIPO plan fails to protect fundamental free-speech interests including parody, and criticism of corporations;
- * Zero Privacy. The WIPO plan provides zero privacy protections

for the

name, address and phone number of individual registrants

* Intimidation. The WIPO plan creates an expensive loser-pays arbitration

process with uncertain rules that will intimidate persons who have

registered into surrendering valid registrations

* Tilts the playing field. The WIPO plan would always allow challengers

to domain names registrations to appeal to a court, but would often deny

this privilege to the original registrant

* Smorgasbord approach to law. Instead of directing arbitrators to apply

applicable law, WIPO proposes using additional, different, rules it

selected-rules that will often disadvantage registrants.

A brief memo explaining these points follows. A more detailed, 50-page

version, is also available in various file formats from

<http://www.law.miami.edu/~amf> . This paper also proposes an alternate,

fairer, reform plan.

The key elements of the simpler reform plan are:

* Reduce speculative registration: Require advance payment before registration

* Penalize false contact details: De-register domains with fake contact information

* Consider creating special rules to penalize large-scale domain speculation

* Trust courts to continue to clarify relevant law

* Understand that rapid changes in technology may make domain names less important

* Create differentiated commercial and non-commercial top-level domains

Lance J. Hoffman, Director, Cyberspace Policy Institute,
Professor EECS

The George Washington University, Washington DC 20052. Phone
(202) 994-5513

⚡ Bringing Y2K fears to a new high -- or low

"Michael P. Gerlek" <mpg@flaxen.com>

Tue, 09 Mar 1999 08:18:00 -0800

From this week's *Infoworld*, in an article entitled 'Planning Beyond Y2K Disruptions':

"People act on fear a lot, and in fear there may be a financial impact. We don't want people going and buying generators when they should be out buying jeans."

-- Director of the Year-2000 project for Levi Strauss

While this does make some sense from a purely business perspective, that it nonetheless is reaching anyone's radar screen makes me a lot more nervous about people reacting to Y2K fears than I am about Y2K itself.

Michael P. Gerlek / mpg@flaxen.com

⚡ Regular break-ins at the Pentagon?

Martin Ward <Martin.Ward@SMLtd.Com>

Mon, 8 Mar 1999 10:33:08 GMT

A report from Edupage:

- > The Pentagon says that defense analysts have successfully thwarted new and
- > recent attempts to break into open Pentagon networks on the Internet. A
- > Pentagon spokesman admits, "There are literally hundreds of

attempts weekly
> to break into the computers. It's a constant because there's
a certain
> cachet to getting into the Pentagon system." The Department
of Defense
> insists that 99.95% of hacking attempts fail to penetrate
beyond the open
> networks and pose no national security threat. (*The New York
Times*,
> 5 Mar 1999)

So there are hundreds of attempts per week and 99.95% of them
fail. Let's
assume about 200 attempts per week. That means, by my
calculations, there
are about five *successful* attempts to break in to Pentagon
systems every
year.

Sometimes, 99.95% success just isn't good enough.

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/>

[Amazingly, Prentiss Riddle <riddle@rice.edu> came up with
EXACTLY
the same numbers and the same conclusion. Unfortunately, the
standard
response seems to be to "blame the hackers" (e.g., Cloverdale)
rather than
to strive for systems that are significantly more secure! PGN]

✶ Re: Remote surgery (Rhodes, [RISKS-20.23](#))

"Dr Declan O'Kane" <dokane@dial.pipex.com>
Wed, 3 Mar 1999 17:57:54 -0000

One issue with surgery-by-wire is that who is legally accountable if a viscus is accidentally perforated or an artery accidentally cut ? Will surgeons blame their network connections ? Will we see Dr X and a Network company being sued for medical malpractice ?

I would feel far more comfortable with an average surgeon with his/her hands inside me than an expert at the end of a long wire ! Another example of technology looking for an application.

Declan O'Kane MRCP(UK)

More on-line trauma

<JJSantos@aol.com>

Thu, 4 Mar 1999 19:28:20 EST

I had an interesting experience happen to me that shook the foundations of my trust in my online experience.

I'm an AOL user. (Now before my elitist compatriots cry out - I have been on the internet from the days of FTP and gopher - local access #s make AOL convenient). I recently logged on to find a message in my inbox titled "requested info"; expecting another spam, I was surprised to find one word in its contents - my password. Yes - access to online banking, funds, accounts, e-zines, and so on. The return address was an AOL domain. Less than a minute after opening the message, I was "Instant Messaged" by someone ("Bob SiteOp") claiming to be an AOL employee, asking whether I

received the
"requested info" message, and asking me to repeat its contents.
Of course,
I didn't bite (or should that be byte?).

After a few phone calls and messages to AOL to report the
matter, most of
the front line phone attendants would either chalk it up to a
virus/trojan
horse, or claim that the situation I described was impossible --
"AOL
doesn't keep passwords on a file". yeah. I finally clamored
enough to get
a supervisor that recognized the seriousness of the situation.
Haven't
heard a thing since she took the info and promised to followup.

A couple of points here; clearly - a serious breach of AOL
security took
place; I've narrowed it down to their Instant Messaging 3rd
party software,
and an auto attendant mail feature. The person who instant
messed me was
clearly in on this scam, and operates on the net out of small
business in
New Jersey (either legitimately or illegitimately).
Unfortunately, since
AOL doesn't have "standardized" id (or screen) names (or a way of
authenticating who is at the other end), from that point on I
was very
uncomfortable messaging ANYONE - AOL or not --- who do you
really know who
you are talking to? Switching to the phone, I thought, would
alleviate that
fear. But after a few calls, subsequent AOL employees would
tell me that
the prior employees I spoke to couldn't have been employees
(based on the
name I was given), or were at least not giving me correct
information. A
slippery slope of trust -- who DO YOU believe?

In the meantime, I've changed my passwords (regularly), "Bob

Siteop"

continues to prowl the electronic alleys for prey, and I've become one computer professional that is beginning to ask himself "what have we wrought?".

✂ Re: Lack of Anonymity in Microsoft Word

Yvo Desmedt <desmedt@cs.uwm.edu>

Thu, 11 Mar 1999 18:48:41 +0900 (JST)

You probably heard that Microsoft Word adds information in the document that can uniquely identify the author, see e.g.:

<http://cnn.com/TECH/computing/9903/08/microsoft.privacy.02/index.html>

At the 1996 Information Hiding workshop, I predicted such a danger. See the second paragraph of Section 3 "Covert identification" starting with "First, any technique using covert channels ..." in the paper

ESTABLISHING BIG BROTHER USING COVERT CHANNELS AND OTHER COVERT TECHNIQUES

which is available from

<http://www.cs.uwm.edu/~desmedt/topics-covert.html>

I welcome any comments. Yvo

✂ Re: Write-protectable hard-drives (Cargill, [RISKS-20.21](#))

Richard Schroepfel <rsc@cheltenham.cs.arizona.edu>

Wed, 3 Mar 1999 08:52:36 -0700 (MST)

A write protect button-toggle-switch was standard on disk drives for the (c. 1975) Digital PDP10 systems. The switch prevented the disk write-head from carrying current. The TOPS-10 operating system supported the feature, allowing the operator to declare drives read-only, or change the software setting. The OS couldn't read the physical switch, and could be confused by operator error: if a drive was physically read-only, but the OS thought it was writable, reading a file would cause the OS to try to update the most-recent-access time in the directory.

None of the hard disks I presently use has a write-protect switch.

Rich Schroepfel rsc@cs.arizona.edu

⚡ Networking'99--NetAdmins & SysAdmins Share Solutions

<enotify@usenix.org>

Wed, 10 Mar 1999 03:58:43 -0800 (PST)

CONFERENCE ON NETWORK ADMINISTRATION
Wednesday and Thursday, April 7-8, 1999

NETWORKING TUTORIAL PROGRAM
Friday and Saturday, April 9-10, 1999

WORKSHOP ON INTRUSION DETECTION AND NETWORK MONITORING
Sunday and Monday, April 11-12, 1999

For the full tutorial and technical program, and online

registration, <http://www.usenix.org/networking99>

Sponsored by USENIX, the Advanced Computing Systems Association
Co-Sponsored by SAGE, the System Administrators Guild
Co-located at Santa Clara Marriott Hotel, Santa Clara,
California, USA

⚡ Workshop on Countering Cyber-Terrorism

Clifford Neuman <bcn@ISI.EDU>

Wed, 10 Mar 1999 20:18:55 -0800 (PST)

Countering Cyber-Terrorism

June 22-23

Marina del Rey, California

A workshop sponsored by the Information Sciences Institute
of the University of Southern California

Please check the web page <http://www.isi.edu/cctws> for more
information, including a position paper from the organizers
which will
be available two weeks prior to the submission deadline.

Organizer's Paper Available	April 5, 1999
Position Papers Due	April 19, 1999

Organizing Committee:

Bob Balzer, Information Sciences Institute, Balzer@isi.edu

Thomas Longstaff, CERT Coordination Center, tal@cert.org

Don Faatz, the MITRE Corporation, dfaatz@mitre.org

Clifford Neuman, Information Sciences Institute, bcn@isi.edu

⚡ PDPTA'99 on Fault Tolerance and Reconfiguration in Distributed Systems

pradip srimani <srimani@CS.ColoState.EDU>

Sat, 27 Feb 1999 09:01:37 -0700 (MST)

Call for Papers for a Special Session on
Fault Tolerance and Reconfiguration in Distributed
Systems

Las Vegas, Nevada, USA, June 30 - July 2, 1999
International Conference on Parallel and Distributed
Processing

Techniques and Applications (PDPTA'99, 28 Jun -- 1 Jul
1999)

<http://www.cs.colostate.edu:80/~srimani/pdpta99.html>

The focus of this special session will be on fault-tolerance
issues of
distributed enterprise systems for time-critical and computation-
intensive
applications. Send extended abstracts by 15 Mar 1999 to

Shahram Latifi
Department of Electrical and
Computer Science
Computer Engineering
University
University of Nevada, Las Vegas
Las Vegas, NV 89154-4026
E-mail: latifi@ee.unlv.edu

EDU

Voice: (702) 895-4016
Fax: (702) 895-4075

Pradip K Srimani
Department of
Colorado State
Ft. Collins
CO 80523 USA
srimani@CS.ColoState.

Voice: (970) 491-7097
Fax: (970) 491-2466

FMICS4

Diego Latella <d.latella@cnuce.cnr.it>
Sun, 7 Mar 1999 18:10:47 +0100 (MET)

ERCIM

Working Group on Formal Methods for Industrial Critical
Systems

Fourth International Workshop

on
Formal Methods for Industrial Critical Systems
July 11-12 1999

Deadline for submission: March 30th, 1999

The Fourth International Workshop on Formal Methods for Industrial Critical Systems will take place in Trento on July 11-12, 1999, as a satellite meeting of FLoC'99 (<http://www.cs.bell-labs.com/cm/cs/what/floc99/>)

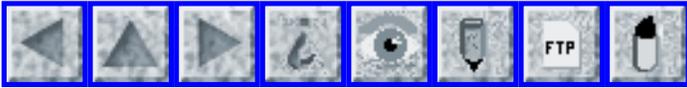
Authors are invited to send their papers to:

S. Gnesi, CNR-IEI, Via S. Maria 46, I56126 Pisa - ITALY phone: +39 050 593489

<http://www.cnuce.pi.cnr.it/cnuweb/research/resgroups/conc-meth/FMICS/WS/Trento99/workshop.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 20: Issue 25

Saturday 20 March 1999

Contents

- [Risks of upgrades involving e-mail](#)
[PGN](#)
- [Satellite outage cuts news service](#)
[Edelson Doneel](#)
- [Great moments in e-mail history](#)
[Lloyd Wood](#)
- [Power outage leaves hospitals in the dark](#)
[Dave Weingart](#)
- [3 patients die when Russian hospital omits utility payments](#)
[Keith A Rhodes](#)
- [Erasable "cash"](#)
[Alpha Lau](#)
- [Windows Registration Wizard may violate European Privacy Laws](#)
[Martin Minow](#)
- [MS Word98 privacy issues](#)
[Chiaki Ishikawa](#)
- [Y2K is the least of it](#)
[Bob Frankston](#)
- [Sri Lankan Banks to close on 31 Dec 1999 for Y2K tests](#)
[Matthew Todd](#)
- [Coming to terms with "bytes"](#)
[Edupage](#)

- [Signs of the times](#)
[Stuart Lynne](#)
 - [Treating names as abbreviations](#)
[Nick Atty](#)
 - [Banks warn public about Y2K scam](#)
[Elliot Silver](#)
 - [H-1 California DOL system crash! Help!](#)
[Anthony Nudelman via Jason Steffler](#)
 - [Re: As we approach April Fool's Day ...](#)
[Jonathan de Boyne Pollard](#)
 - [They threatened, and apparently they have followed through ...](#)
[Fred Cohen](#)
 - [REVIEW: "Time Based Security", Winn Schwartau, 1999](#)
[Rob Slade](#)
 - [CFP: ISOC Year 2000 Network & Distr. System Security](#)
[David M. Balenson](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Risks of upgrades involving e-mail

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

Wed, 17 Mar 99 17:03:00 PST

Our CSL majordomo server was apparently blown away by the installation of a new version of sendmail. If you received a bounce on a subscription change request on the Ides of March (Monday 15 Mar), or if you requested a change but this issue is still using your old address, please try again. TNX. PGN

Beginning last Friday, an enormous number of pieces of mail on a private distribution to me at sri.com rather than the customary CSL found their way into a black hole as the result of a seemingly harmless DNS upgrade made by the sys admins at sri.com. Fortunately, someone deduced that I was not

responding, which triggered the discovery and temporary fixing of the otherwise undetectable problem (there were no bounces, just bit-buckets).

I am told that the fix will go away on the next upgrade, so please use only my CSL address.

Once again we are reminded of the incredible variety of risks of e-mail.

✂ Satellite outage cuts news service

"Edelson, Doneel" <doneeledelson@aciins.com>

Fri, 12 Mar 1999 12:17:24 -0500

North American operations of the Associated Press (among others) were affected on 12 Mar 1999 by the failure of a GE-3 satellite, which is spinning out of control. [Source: *USA Today*, 12 Mar 1999]

[A Reuters item in *The Washington Post*, 15 Mar 1999, reported that

service was out for almost 6 hours, and is now back to normal. The cause

was not given. Reported to RISKS by Paul Walczak. PGN]

✂ Great moments in e-mail history

Lloyd Wood <eep1lw@surrey.ac.uk>

Mon, 15 Mar 1999 02:28:05 +0000 (BST)

<http://www.usnews.com/usnews/issue/990322/22hist.htm>

(Cover story 22 Mar 1999 on a partial history of e-mail)

OCTOBER 1969:

Leonard Kleinrock, a UCLA computer science professor, sends the first e-mail message to a colleague at Stanford. The computer promptly crashes.

-- and nothing much has changed since.
amusing list, btw. worth a look.

[Well, it was certainly not the FIRST e-mail message, but it might well

have been the first ARPAnet e-mail message. USNews should add earlier

items, such as the CTSS e-mail system written by Tom Van Vleck and Noel

Morris, which I used during the early Multics days in 1965, and it apparently did **not** cause any crashes. An paper reference is found in

CTSS Programming Staff Note 39 by Glenda Schroeder, Louis Pouzin, and Pat Crisman, undated, but it was prior to PSN 40, which was dated

8 Jan 1965. RISKS will be happy to set the record straight on any earlier e-mail systems, in the RISKS-of-historical-inaccuracies department. PGN]

⚡ Power outage leaves hospitals in the dark

Dave Weingart <dweingart@chi.com>

Fri, 12 Mar 1999 09:59:47 -0500

On Wednesday, March 10, 1999, two of the three hospitals that make up Long

Island Jewish Medical Center in Long Island, NY were without power for a

period of 47 minutes, starting at 5:58pm. Patient care was apparently not

impacted, although 2 operations were completed by battery operated lights

and bags of ice were hauled from the cafeteria to the blood bank to keep

things cold. Life support equipment has an internal battery backup and kept

functioning during the outage.

Investigations are underway to determine none of the four backup generators

worked.

Kids, let this be a lesson. It's not enough to have a backup system in place...you need to make sure it will work when needed.

Dave Weingart, Randstad North America dweingart@chi.com 1-516-682-1470

⚡ 3 patients die when Russian hospital omits utility payments

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

Fri, 12 Mar 1999 07:16:46 -0500

Three patients on intensive-care life support died on 11 Mar 1999 in a Siberian hospital in Prokopiyeysk (Kuzbass) because the local electricity company cut the power after warnings over unpaid bills. [Source: Agence

France-Press, 11 Mar 1999; PGN-ed]

[Just a note to show, again, that Y2K is not the only issue in Russia. KAR]

⚡ Erasable "cash"

Alpha Lau - EPA/D/N <alpha.lau@ericsson.com.au>

Fri, 12 Mar 1999 16:24:03 +1100

Wired News (<http://www.wired.com/news/news/technology/story/18401.html>)

reports that Berlin subways will be using Motorola's Venus SmartCards as tickets for travel. The smartcards have up to 32kbytes of EEPROM (electrically erasable read-only memory).

Would it be a risk for static discharge to wipe the EEPROM, thus losing all your "cash"? Any cases of this sort reported?

Alpha Lau, Ericsson Australia, Network Systems GPO Box 256C
Melbourne VIC 3001
alpha.lau@ericsson.com.au MC34.22 ph: +61 3 9301 6197

[That would be a case of U-Bahn-ic plague! PGN]

✂ Windows Registration Wizard may violate European Privacy Laws

Martin Minow <minow@apple.com>

Fri, 19 Mar 1999 14:20:18 -0800

An item in The Register <<http://www.theregister.co.uk/990319-000002.html>>

notes that the personal data sent to Microsoft by the Windows 98 registration wizard may be in breach of European privacy legislations. The Swedish Computer Inspectorate is reportedly considering an investigation.

[So, we can wait for the Expectorate? PGN]

In a related matter, Jason Catlett of the Junkbusters privacy lobby has filed a formal complaint about Microsoft with TrustE, the voluntary American computer privacy auditing organization. The Register notes: "But TrustE is a Microsoft corporate partner, and gets \$100,000 a year from Redmond. Tricky - the company intends to say what it's going to do about this particular hot potato today [March 19, 1999]".

Transcribed and summarized by Martin Minow, minow@pobox.com

✂ MS Word98 privacy issues

Chiaki Ishikawa <Chiaki.Ishikawa@personal-media.co.jp>

Fri, 19 Mar 1999 21:43:00 +0900 (JST)

A reporter's summary of MS-Word98 and MS-office98 in general can be found at

<http://www.macintouch.com/o98securitysamp.html>

In the same page, there are comments from the readers. Some mention that they can find information such as credit card #, directory names where important files are kept, etc. that they think should not be in the files.

I think some of these observations are due to the re-use of old file blocks without clearing the file blocks first.

In any case, it is a little disturbing to think that '1984' has arrived without much fanfare. [Surprised? RISKS began in 1985, and we observed early-on that it was already here.

PGN]

Chiaki.Ishikawa@personal-media.co.jp.NoSpam
Personal Media Corp., Shinagawa, Tokyo, Japan 142-0051

✶ Y2K is the least of it

"Bob Frankston" <BobFrankston@Mediaone.net>

Fri, 19 Mar 1999 02:13:45 -0500

I just got off the phone with support line of the remaining Boston Bank (no need to name it except for those who don't know about Fleet taking over BankBoston). Their home banking does not work with Internet Explorer 5. This would be understandable if they had tested and discovered a new problem with the retail release or if Microsoft hadn't mentioned that a new release was coming out.

But, in December, I had a long e-mail exchange when IE5 suddenly stopped working with their service and the response was that they didn't support unreleased browsers and weren't even curious about why it might have stopped working.

Today I had two conversations with their support staff. During the first one they basically said it was Microsoft's fault because they released a new browser. I presume they'll blame the Pope for surprising them with the year 2000. They also made up excuses such as IE5 not having 128 bit security, which was totally bogus.

Even if any of this were true, it is still the bank's fault since if were is an IE5 problem, they should simply produce a message saying the browser is not supported instead of simply going mute.

I then looked at the code. If I read it correctly, the progress messages are completely bogus and are generated by a local timing loop purely to pacifier the user. More striking was that the body of the message looked like the boiler plate for the web page. It seems as if the server explicitly checks for the browser version and produces browser-specific HTML. For IE5, it seems to fall through to the template code but there is no error checking. I called back and spoke to a supervisor who accepted my analysis, but there wasn't much he could do about it. At least, it reduced my hostility.

This is very disturbing since it is so trivial and obvious and, even more so, something I had reported in December. Unlike the subtle bugs often reported here, this is simply stupid and inexcusable. There doesn't

seem to
be much connection between the support staff and the backroom. It is
very
embarrassing since it is so visible and unnecessary. Even more so
since the
IE4 support simply worked in IE5 and someone had to explicitly break
the
support on (or about) December 28, 1998.

Sadly, this will soon be the last of the larger banks in Boston ...
IE5
does work with BankBoston.

Bob Frankston <http://www.Frankston.com>

🚩 Sri Lankan Banks to close on 31 Dec 1999 for Y2K tests

"Matthew Todd" <matthew@mail.cmb.ac.lk>

Fri, 19 Mar 1999 11:27:09 +0600

Central Bank has decided to close all banks to the public December
31 this
year to do the final assessment on all computer systems compliance
to the
Year 2000 (Y2K) problem. [Beginning of an item in *The Island*, 12
Mar
1999, noting that employees will be at work. PGN-ed]

Risks:

1. December 31 appears to be a little late for final testing of Y2K
readiness. What if something isn't ready? Oh, well there'll still be
the
weekend to fix it I suppose!
2. The contingency plan to close on December 30 as well would seem
to be
superfluous. Will the decision to close then be made half way through
testing on 31st when they realise they don't have enough time?
3. Moving the deadline from March 31 to June 30 would also appear to
be a

time waster. What will happen if some banks are still lagging behind in June, will the deadline move again? Will it keep moving until it reaches December 31? That's one deadline which won't move!

4. That some bankers were not even aware of the Y2K problem is beyond belief. Which banks? I want my money out now!

5. The CEB is only testing power plants they suspect aren't compliant. What about the rest?

6. [Power plant] Sapugaskanda was confirmed as compliant, but won't work after 2001. How many other power plants around the world will fail on January 1, 2002?

7. The operating system is too advanced for the local staff. What more can I say?

✈ Coming to terms with "bytes"

Edupage Editors <edupage@franklin.oit.unc.edu>
Tue, 16 Mar 1999 11:21:15 -0500 (EST)

Computer terminology is becoming more precise: the International Electrotechnical Commission, which creates standards for electronic technologies, is adopting new prefixes to describe data values. The new term "kibibyte" will more accurately describe the number of bytes in a kilobyte -- rather than being 1,000, as could be inferred by the prefix "kilo," a kilobyte actually has 1,024 (2 to the 10th power) bytes. The metric prefixes currently employed -- kilo, mega, giga, etc. -- accumulate as a power of 10, rather than the binary system used in computer code.

Thus, the Commission will use kibi, mebi, gibi, tebi, pebi and exbi to express exponentially increasing binary multiples (2 to the 10th power, 2 to the 20th power, etc.). "There was a need to straighten this out," says Barry Taylor of the National Institute of Standards and Technology. (*Science*, 12 Mar 1999; Edupage, 16 March 1999)

[This may lead to kibi-tsars, mebi-or-mebi-not, gibi-ous moonings, tele-tebi, pebi-le-mocha, and exbi-gated Websites. (Garrulous in the NIST?)

But, following on an earlier observation from Peter and Dorothy Denning,

it does create a new solution to the Y2K problem:

Change K from kilo to kibi, which puts the problem off until 2048. PGN]

<REMINDER to the media: PLEASE STOP calling it the Millennium Bug.

It is a really a collection of design flaws and not just a program

bug, and it is not the end of the Millennium, for which we have to

wait until "1/1/01"!> PGN]

✶ Signs of the times

Stuart Lynne <sl@fireplug.net>

Thu, 11 Mar 1999 12:33:11 -0800

Port Moody, BC, (where I currently reside) installed some nice "Welcome to..." signs a few years ago. They incorporate a nice little automated light display which typically is used to tell us about upcoming local events.

For the last month or so, one sign has been consistently displaying "NO CARRIER". Which probably gives us some indication about how these are getting their daily dose of information.

Wonder if the modem is fried or did someone forget to pay the phone bill?

Stuart Lynne <sl@fireplug.net> 1-604-461-7532 <<http://edge.fireplug.net>>

[Carrier is a major producer of air conditioning. In that the air in

Port Moody obviously does not need conditioning, I'd like to imagine that

the sign was hacked by the Carrier Corporation in protest. But more

likely, the sign is programmed to grab the message of the day remotely and

could not connect. PGN]

✂ Treating names as abbreviations

Nick Atty <nick@nandj.freemove.co.uk>

Fri, 19 Mar 1999 20:41:15 GMT

About a year or so ago, I got a letter from the marketing department of

British Gas (with whom I have a gas account) addressed to me as "Mr Attorney". My bills arrived correctly addressed to "Mr Atty". I subsequently discovered my father had had a similarly addressed letter.

This summer I moved house, and moved my gas account. Properly addressed

bills arrived. Then, last week, a marketing letter arrived for "Mr Attorney".

So, somewhere inside British Gas is something that transfers names and

addresses from their billing system to their marketing system. And for some

incomprehensible reason, it treats people's names as abbreviations and

expands them. And what is even odder, it doesn't expand titles

("Mr" rather than "Mister". The fact I'm "Dr", and have told them so, is a side issue).

Overseas readers should note that "Atty" is not used in Britain for "Attorney" - I'd never come across it in my life until I started to use the internet. So anyone else with my (rare) surname could be utterly confused.

Needless to say, the letter completely fails in persuading me I should let them anywhere near my heating system. And I've had a lot of fun wondering just what it does to other people's names.

Nick Atty

⚡ Banks warn public about Y2K scam

Elliot Silver <elliott@ali.bc.ca>

Thu, 18 Mar 1999 13:14:38 -0800

Following up on the recent discussion of Y2K fraud, readers might find this URL of some interest.

http://www.cba.ca/eng/Media_Centre/Press/990309-a.htm

It describes a telephone scam where the caller identifies himself as a bank employee, and requests personal account information to help verify their Y2K testing.

Elliot Silver, ALI Technologies Ltd., 95 - 10551 Shellbridge Way
Richmond, BC, CANADA V6X 2W9 604/279-5422 x376 elliott@alitech.com

⚡ H-1 California DOL system crash! Help!

Jason Steffler <jagwar@nls.net.removeMe.org>

Thu, 18 Mar 1999 20:56:56 -0500

Anthony Nudelman <no.spam@tecsi.com> writes:

> This is an update about California, taken from

> <http://www.immigration-lawyer.com/news/DOL.htm>

>

> CALIFORNIA LCAs RE-ROUTED TO DOL/WASHINGTON, DC

> 5 Mar 1999 (report from AILA)

> Due to a severe breakdown in Region IX's computer system, LCAs
(for H1B

> petitions) and labor certifications have been at a complete
standstill.

> After extensive negotiations, AILA liaison attorneys report that
the

> problem has been temporarily resolved by electronically filing
these

> Region IX petitions at the DOL office in Washington. LCAs caught
in the

> backlog can be refiled to the electronic system at DOL
headquarters.

Jason Steffler

🔥 Re: As we approach April Fool's Day, ...

<Jonathan_de_Boyne_Pollard@jba.co.uk>

Tue, 16 Mar 1999 14:37:50 +0000

Re: Neumann, [RISKS 20.24](#) and Minow [RISKS 20.23](#)

PGN> As we approach April Fool's Day, it seems to be more difficult
to
separate the wheat from the chaff, as in the case of "Mobile phones
cause
memory loss" in [RISKS-20.23](#), which is speculative at best.

The article in The Register referenced by Martin Minow was vague,
but
that, it seems, was a deliberate joke, changing names and places each

paragraph and repeating itself to make the reader think that they had used their mobile 'phone too much! The story does not seem to be a fabrication, though. More serious articles on this topic, with more information, can be found at the BBC News site:

<http://news.bbc.co.uk/hi/english/health/newsid%5F288000/288245.stm>

"Scientists cut their mobile phone use" (1999-03-01)

Colin Blakemore, Waynflete professor of physiology at Oxford University, is reported as having cut back on his own use of mobile telephones, and speculating upon short-term and localised effects of microwave radiation near certain parts of the brain; but is also reported as saying that reports that suggest that mobile telephones could cause permanent damage should be treated with caution. Some of the pertinent details missing from or not clear in the article in The Register are that the research that sparked the story was carried out at Bristol Royal Infirmary, by a team led by Dr Alan Preece, and that it will be published in April in the International Journal of Radiation Biology. (Does the IJRB publish April Fool articles?) The article also includes quotes from the National Radiological Protection Board and spokesmen for the mobile telephone industry.

<http://news.bbc.co.uk/hi/english/health/newsid%5F296000/296976.stm>

"Mobile phone caused brain damage, claims man" (1999-01-15)

A former BT engineer is suing BT for damages of up to =A3 100,000, claiming short term memory problems as a result of being required to use a mobile telephone for up to 90 minutes. More quotes from the NRPB.

⚡ They threatened, and apparently they have followed through ...

Fred Cohen <fc@all.net>

Sat, 13 Mar 1999 21:14:10 -0800 (PST)

I just got this happy note from a sender who will remain anonymous for obvious reasons. Before continuing on, the reader should be aware of the previous threats made by several virus writers associated with codebreakers.org (published in a recent Risks) who were offended by the fact that their ISP decided to shut their site down. They believe that I caused this to happen and have decided to get even by associating my name and Web site with the virus.

I did not write the virus and it has never been to my Web site or on any of my systems (I don't run Excel or Word).

FC

> Here's a message (see below) I have just posted to the following three
> newsgroups: [...] concerning two word documents which I downloaded
> containing a virus. The file information for both documents listed the
> author as Fred Cohen and the corresponding website as www.all.net
> Just thought you might be interested to be informed. Perhaps if Mr Cohen
> wasn't the perpetrator of the virus himself, then perhaps he should be
> aware that his system has picked it up from somewhere and passed it on!
>
> N
>
>
=====

>
> I recently (& stupidly?) downloaded two Word documents from, I think, one of
> these newsgroups, which supposedly gave details of adult site passwords.
> (Contents of files repeated below - both were the same.)
>

> Although I subsequently deleted these files, my copy of Norton
AntiVirus
> (armed with the latest set of virus definitions dated 8 March
1999) later
> detected that these files were infected with a virus. (It detected
them
> because, although deleted, they were still present temporarily in
the Norton
> protected recycle bin.)
>
> The virus is called 097M.Jerk and is a Polymorphic macro virus
which infects
> Excel97 and Word97 files. There are apparently two variants, both
of which
> causing a message to be displayed in May/June I think.
>
> Just to warn anyone who might have downloaded these documents
also! Beware!
>
> N
>
[Contents of the doc file omitted. PGN]

Fred Cohen & Associates: <http://all.net> - fc@all.net - tel/fax:925-454-0171

[Fred's extensive disclaimer omitted, as per RISKS policy.]

🔥 REVIEW: "Time Based Security", Winn Schwartau, 1999

Rob Slade <rslade@sprint.ca>

Fri, 19 Mar 1999 10:06:34 -0800

BKTMBSSC.RVW 990212

"Time Based Security", Winn Schwartau, 1999, 0-9628700-4-8, U\$25.00/C\$37.00

%A Winn Schwartau winnschwartau@infowar.com

%C 11511 Pine St. N., Seminole, FL 34642

%D 1999

%G 0-9628700-4-8

%I Inter.Pact Press

%O U\$25.00/C\$37.00 813-393-6600 fax: 813-393-6361

%P 174 p.
%T "Time Based Security"

The idea is simple, and even elegant. Given enough time and resources, somebody is going to be able to crack whatever security you put in place. Therefore, instead of building ever bigger and more imposing (and expensive) walls, balance how long it will take someone to get through the wall against how long it will take you to figure out that digging is going on and how long it will take you to stick a fire hose down a putative gopher hole.

The idea isn't, of course, radically new. Community policing officers have been saying the same thing in public security seminars for years. Make the bad guy take longer to get in, and you'll have more time for someone to notice, or for us to get there.

Implementation, though, is not quite so simple. Especially when you are dealing with something as complex as a publicly accessible and networked computer system.

Chapter one is a general promotion for the Time Based Security (TBS) model, which hasn't been presented yet. The introduction's cry that we never have enough time and have to move ever faster is reiterated in chapter two, along with another assurance that Time Based Security is what we need. The demise of the big, limited, simple to protect computer is bemoaned in chapter three. Chapter four says that the fortress mentality never did work, and besides, we want people (some people) to access our systems for some purposes. (Were it not for the fact that the chapters are so short, and the vague idea that we are getting closer to TBS, I would be getting a little impatient about now.) Sorry, but chapter five goes into the shortest history of computer security I think I've ever seen, six says it didn't work, and seven runs us right back to Jesse James. But by the end of chapter seven, we are at least pointed in the right direction: the security of a container is a comparison between the time the bad guys need to get in, and the time the good guys need to get there. This is repeated in a different form in chapter eight. Chapters nine to eleven repeatedly

formularize this, pointing out that you need to measure your protection in terms of time to fail, and that the time taken to detect a problem, plus the time taken to effectively respond to it, must be less than the time the protection provides. Schwartau gets into a lot more detail, though for only one situation, with a questionnaire in chapter twelve.

Chapter thirteen starts to get into the complexity of things, looking at the variable amounts of damage that can be done in a given amount of time. Fourteen looks at costs of attacks while fifteen talks about the value of data. The title of chapter sixteen seems to indicate that some things don't need protecting, while the content looks more like some things cannot be exposed to any level of risk. Recursion of detection is promoted in seventeen. I think that chapter eighteen is suggesting that you use multiple barriers to stop intruders. But I'm not very sure of that. Nineteen and twenty seem to be saying that you should protect vital points with greater security, and try to avoid "single points of failure."

Chapter twenty one looks at improving the reaction time. Twenty two stresses the importance of taking a long time to look at all the options in order to assess your security. (This is in rather stark contradiction to the promises on the cover and in the introduction that TBS was going to provide a shortcut.) A few options to increase protection get some detail in twenty three while increased detection is looked at in twenty four. A metric is achievable with TBS, but chapter twenty five does rather gloss over the work you will have to go to in order to accomplish it.

Chapter twenty six talks about denial of service, but does not really integrate it with the TBS concept. Some infowar classes are used to repeat the adjuration to put protection where it is most needed in chapter twenty seven. Twenty eight suggests that deception is a good protective tool. (Sounds just a tad like security by obscurity, but we'll let it go, shall we?) The final chapter again promises that TBS will give you measurable security.

The concept is sound. The implementation is left as an exercise to the

reader.

copyright Robert M. Slade, 1999 BKTMBSSC.RVW 990212
rslade@vcn.bc.ca rslade@sprint.ca robertslade@usa.net pl@canada.
com
<http://victoria.tc.ca/techrev~rslade> or <http://sun.soci.niu.edu/~rslade>

✦ CFP: ISOC Year 2000 Network & Distr. System Security (NDSS 2000)

"David M. Balenson" <balenson@tislabs.com>

Wed, 17 Mar 1999 13:18:44 -0500

C A L L F O R P A P E R S
The Internet Society
Year 2000 Network and Distributed System Security
Symposium (NDSS 2000)
Catamaran Resort Hotel, San Diego, California
2-4 February 2000

Dates, final call for papers, advance program, and registration information will be available soon at <http://www.isoc.org/ndss2000>. Paper and panel submissions due 16 Jun 1999.

GENERAL CHAIR:

Stephen Welke, Trusted Computer Solutions

PROGRAM CO-CHAIRS:

Gene Tsudik, USC / Information Sciences Institute

USC Information Sciences Institute, 4676 Admiralty Way,

Marina Del Rey, CA 90292, ndss00@isi.edu

TEL: +1 (310) 822-1511 ext 329, FAX: +1 (310) 823-6714

Avi Rubin, AT&T Labs - Research

Publ: David M. Balenson, Cryptographic Technologies Group, TIS Labs at Network

Associates, Inc. 3060 Washington Road #100, Glenwood, MD 21738 1-443-259-2358

[NDSS 1999 was a really fine conference. Support your ISOC. 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 20: Issue 26

Thursday 1 April 1999

Contents

- [The Y9Z Problem](#)
[Mark Thorson](#)
- [Yet another Y2K debacle](#)
[Jon Loux](#)
- [Vatican announces all computer systems ready for new millennium](#)
[Matthew Todd](#)
- [Y10K opportunity](#)
[Matthew Todd](#)
- [Torvalds, SlashDot, and Stallman](#)
[Martin Minow](#)
- [Melissa and RISKS](#)
[PGN](#)
- [Melissa macro virus](#)
[Rob Slade](#)
- [Melissa and monoculture](#)
[Nick Leverton](#)
- [Melissa and GUIDs](#)
[Ronan Waide](#)
- [Melissa + meme = future disaster](#)
[Bear Giles](#)

✶ The Y9Z Problem

Mark Thorson <eee@netcom.com>

Sun, 14 Mar 1999 17:20:29 -0800 (PST)

In my extensive consulting work on the Y2K problem, a new problem has come to my attention. One thing all of my clients have in common is that we are forbidden from touching the database format -- only the source code may be modified. Further, we use formal methods for proof of program correctness, so any change we make actually costs more to verify than to develop the change itself.

Because of these restrictions, all of my clients have opted to allow the date field to roll over from 99 to 9A in the year 2000. But this only buys another 26 years of service. What happens in the year 199Z (i. e. 2025 AD)?

Only one client (a company with a strong "do it right the first time" corporate philosophy) has opted to follow my recommendation, which is that the year 199Z be followed by the year 19A0. This buys another 936 years, to the year 19ZZ (i.e. 2961 AD).

Because of the verification requirement, this is more than twice as expensive as the 26-year fix. Rather than doubling the effort required for the single digit, it's more like the effort squared to apply to two digits.

What year follows 19ZZ? My recommendation is that the year 19ZZ

be followed
by the year represented by "2000". If we can't fix the problem
by then, we
deserve the fate of extinction. Hopefully, our bones will serve
as a source
of calcium for whatever superior species comes along to replace
us.

Mark Thorson (eee@netcom.com)

⚡ Yet another Y2K debacle

Jon Loux <JLOUX@UCONNVM.UCONN.EDU>

Mon, 22 Mar 99 08:19:37 EST

I found this in a respected journal of scientific neatstuff.

Researchers Find Y2K Bug in Human Brain!
by Natalie N. Quirer

Researchers at the Yale Neurological Sciences Department
announced today
that they have discovered a millennium bug implanted in the
brains of human
beings. "The brain is just a big computer, like any other,"
says Dr. Uri
Ignoramus of the Synaptic Research Lab. "It has to keep track
of times and
dates. Like when you wake up just before your alarm clock or
remember your
mother's birthday a day late. Stuff like that."

According to researchers, when the clock strikes midnight in
January 2000,
power outages and planes falling from the sky will be the least
of our
worries. Along with such mundane annoyances like frozen bank
accounts and
nuclear detonations, add epileptic like seizures, an
uncontrollable desire

to watch the Rosanne Show, and suddenly not being able to remember where your keys are or why you are living in the same building with that ghastly person.

"Billions of years of evolution," says noted Nobel laureate Albert Bearstein. "You'd think they could have anticipated this sort of thing. Just how did they manage the year 0 rollover, anyway?"

In anticipation of the impending cranial apocalypse, experts insist that the population stay calm. "There is plenty of time for panic later."

In the meantime, stock up on St. John's wort.....

Jon Loux, Data Administration, University of Connecticut

✶ Vatican announces all computer systems ready for new millennium

"Matthew Todd" <matthew@mail.cmb.ac.lk>
Thu, 1 Apr 1999 08:59:26 +0600

Vatican announces all computer systems ready for new millennium

Rome, Washington, London and Delhi, 1 Apr (Reuters) A spokesman for the IT department of one of the world's smallest states, the Vatican City, announced yesterday that all computer systems of the Roman Catholic church world-wide were now ready for the next millennium.

Asked what solution had been used to combat the so-called "Y2K problem", he said that the solution had been simple. "All we did was to

revert to the Roman numbering system. This makes the current year MCMXCIX. Next year will be MM. Since this is shorter than the current representations there will not be a storage problem. Also, since there is no zero in the Roman number system nothing will reset."

The spokesman also pointed out that the absence of a zero also categorically proved the new millennium would begin in MMI. He explained that the zero had been introduced in MCCII by an Italian mathematician called Fibonacci. This explained why there was no confusion at the start of the current millennium in MI.

The church is now considering excommunicating Fibonacci for the confusion he has caused.

Subsequently in Washington, a spokesman for US President Bill Clinton said, "we think that it is harsh to pin the blame on one poor Italian. After all, they are Arabic numbers. Clearly we must break all ties with the Arab world until they hand over those responsible."

"In the past, the number zero was known as a cipher. Clearly this shows that strong cryptography is harmful and the Government must retain control."

In a separate development, Prime Minister Vajpayee of India pointed out that "actually, the number zero was invented in India in about 876AD. Clearly the Arabs and the West have no concept of nothing. Only South Asians can really understand what it means."

It is unclear whether he was trying to say that only the Indian software industry could solve Y2K. It is thought that a case may be brought to WIPO concerning the loss of intellectual property suffered by India for the last DCCC years. Damages could run to billions of dollars.

⚡ Y10K opportunity

"Matthew Todd" <matthew@mail.cmb.ac.lk>

Thu, 1 Apr 1999 09:33:03 +0600

Date: 1 April 9990

> From: System Proving Office and Original Fault Finding,
MacroHard Corporation

To: Bob Gates-Windows-Doors III, CEO MacroHard Corporation

Subject: Y10K

It would seem that a potentially serious fault exists which will affect all known computer systems containing a date processor. This fault could have catastrophic consequences on January 1, 10000. The origin of the fault has been traced to a programming error which originated in the late years of the 20th century, when computing was in its infancy and had not developed into the science which it is today.

It seems that before the historic splitting of the parent company of MacroHard and Microsoft, as ruled by the US Supreme Court, that programmers around the world all mistakenly wrote software using only 4 digits to represent the year. Furthermore, this was then built into the hardware of

the time.

Huge amounts of effort were expended in the early days of computing correcting an even earlier "bug" when only two digits had been used in some systems to represent the year. Why at that time no-one had the foresight to properly correct this error no-one can tell, although speculation rests with some quasi-religious belief that the world would come to an end in the new millennium, so they only had to get through to 2001.

This error has been built into all processing chips of the MacroHard Corporation ever since its formation out of the remains of MS-OS, Intel and AMI following the ruling of the Supreme Court. The effects of this error could be disastrous. On January 1, 10000 all systems containing a MacroHard chip will roll-over to 0000. Due to backward compatibility with MS-DOS this will then be interpreted by the operating system as either January 1, 1980 or January 0, 1900.

Explanation: MS-DOS was the first operating system of the MS organisation and originally did not recognise dates before 1980; when MS introduced its Excel spreadsheet program, only dates after 1900 were recognised as valid dates.

Other problems: Y10K is a leap year, so was 1980, but 1900 wasn't, therefore 29 February, 10000 may cease to exist on some systems. Fortunately, MS foresaw this by including 29 February, 1900 as a valid date in their MS-Excel package.

Note: a similar problem to this was overcome in 2099 by MacroHard, when all processors would have reset themselves to 1980 on January 1, 2100. However, at that time it was still considered adequate to use four digits to represent the year.

MacroHard chips are now embedded in so many systems that control the day to day lives of every citizen in the known universe that urgent action is required. We recommend the establishment of a secret Y10K task force to consider possible options and defence strategies to protect MacroHard Corporation from the potential fallout.

Replacing every single MacroHard chip for free is clearly not an option, as although this would be within the financial means of the company it is against corporate policy. One possible solution, based on the previous history of Microsoft with Y2K is to announce the potential problem, but pin the blame on those who made bad decisions in the past for short-sighted gain. We can then announce a new generation solution, which will be Y10K compliant - possible name: System 10000. This solution can then be sold on the open market. Anyone choosing not to upgrade could be held responsible for the consequences, since we would have given them both adequate warning of the impending disaster, and would have provided an alternative. If we fix the price well in advance we should be able to turn this into a healthy profit making opportunity.

At the moment we have almost 10 years to take advantage of this

opportunity,
so it may still be too early to make an announcement. However,
timing is
critical, since we don't want anyone else to realise this is
going to happen
beforehand or they might try to pin the blame on us.

⚡ **Torvalds, SlashDot, and Stallman**

Martin Minow <minow@apple.com>

Wed, 31 Mar 1999 20:48:35 -0800

<<http://www.salonmagazine.com/21st/>> (good Thursday, April 1)

reports on changes in the software industry: Linus Torvalds
starts

LinusSoft, a for-profit operating system venture (they expect to
file for an

IPO within 36 hours). Also, SlashDot <<http://www slashdot.org>>

(home of many

open-source related flames) launches Slashdot Investor.

Also, "In Redmond, Microsoft announced that Free Software
Foundation founder

Richard Stallman had accepted the new position of Senior Vice
President for
Ideology."

Martin Minow, minow@pobox.com

⚡ **Melissa and RISKS**

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

Tue, 30 Mar 1999 08:01:17 PST

With all the furor since last Friday over the Melissa virus-like
Trojan

hosed e-mail propagation (see next items), deeper issues are somehow lost in the shuffle. The vulnerabilities exploited in the MS Word macro virus in Microsoft Outlook and Outlook Express have been around for a long time and are likely to be around for a long time. Although some palliative fixes are available, the fundamental problems remain. (For example, filters deleting e-mail with "Subject: Important Message from ..." are only partially useful, in light of recent versions of Melissa with blank Subject lines.) The basic system infrastructure is incapable of adequately protecting itself against all kinds of misuses, and this particular exploit is just another reminder that many folks need to wake up. The situation could have been much worse, but unfortunately many folks who depend on systems that are inherently inadequate do not get the proper messages when the situation is **not** a terrible disaster. On the other hand, even if we had terrible disasters, it does not seem to be enough. And this was presumably not even an early April Fool's spoof -- just another example microcosmically of what could be done macrocosmically. Many of the constructive lessons that should have been learned from the Internet Worm over 10 years ago are still unlearned.

[The late-breaking news (31 Dec 1999) that Yugoslav crackers are performing denial-of-service attacks against the NATO Website should also come as no surprise. Can it be that only RISKS readers realize how flaky our communications <*> infrastructures are?]

[* I spent last Saturday at the 70th birthday roast for my PhD thesis professor, Tony Oettinger, who long ago coined the combining term "Communications". In that the string "pun" is contained therein, it seemed appropriate to mention it here. PGN]

✶ Melissa macro virus

Rob Slade <rslade@sprint.ca>
Tue, 30 Mar 1999 16:51:23 -0800

A report prepared by Robert M. Slade

The following is an attempt to bring together the information about the Melissa virus. It is taken from the most reliable available sources. Additional sites have been listed at the end of the article. I have not added a copyright line to this message in order to allow it to be used as needed. I will be posting the latest updated version of this article at <http://sun.soci.niu.edu/~rslade/melissa.txt> and <http://victoria.tc.ca/techrev/melissa.txt>.

The virus, generally referred to as W97M.Melissa.A (with some variations: Symantec, in a rather strained effort to be cute, seems to be calling it "Mailissa"), is a MS Word macro virus. This means that, if you don't use Word, you are safe. Completely safe. (Except for being dependent upon other people who might slow their/your mail server down. More on that later.) If you need to look at MS Word documents, there is a

document

viewer available (free, as it happens) from Microsoft. This viewer will not execute macros, so it is safe from infection.

In the messages about Melissa, there have been many references to the mythical and non-existent "Good Times" virus. Note that simply reading the text of a message still cannot infect you. However, note also that many mailers, in the name of convenience, are becoming more and more automated, and much of this automation concerns running attached files for you. As Padgett Peterson, author of one of the best macro virus protection tools, has stated, "For years we have been saying you could not get a virus just by opening E-Mail. That bug is being fixed."

Melissa does not carry any specifically damaging payload. If the message is triggered there will be text added to the active document. The mailout function can cause a large number of messages to be generated very quickly, and this has caused the shutdown of a number of corporate mail servers.

If you have Word set with macros disabled, then the virus will not active.

However, relying on this protection is a very dangerous proposition.

Previous macro viruses have also killed macro protection in Word, and this one does as well.

The name "Melissa" comes from the class module that contains the virus. The name is also used in the registry flag set by the virus.

The virus is spread, of course, by infected Word documents.

What has made
it the "bug du jour" is that it spreads *itself* via e-mail. We
have known
about viruses being spread as attachments to e-mail for a long
time, and have
been warning people not to execute attachments (or read Word
documents sent
as attachments) if you don't know where they came from. Happy99
is a good
example: it has spread very widely in the past month by sending
itself out
as an e-mail attachment whenever it infects a system.

Melissa was originally posted to the alt.sex newsgroup. At that
time it was
LIST.DOC, and purported to be a list of passwords for sex
sites. I have
seen at least one message theorizing that Melissa is someone's
ill-conceived
punishment for viewers of pornography. This hypothesis is
extremely
unlikely. Sending a virus to a sex related newsgroup seems to
be a reliable
way to ensure that a number of stupid people will read and/or
execute your
program, and start your new virus off with a bang. (No pun
intended.)

If you get a message with a Melissa infected document, and do
whatever you
need to do to "invoke" the attachment, and have Word on your
system as the
default program for .doc files, Word starts up, reads in the
document, and
the macro is ready to start. If you have Word's "macro
security" enabled
(which is not the default) it will tell you that there is a
macro in the
document. Few people understand the import of the warning, and
there is no
distinction between legitimate macros and macro viruses.

Because of a technical different between normal macros and "VBA

objects," if you ask for a list of the macros in the document, Melissa will not show up. It will be visible if you use the Visual Basic Editor, but only after you have loaded the infected file.

Assuming that the macro starts executing, several things happen.

The virus first checks to see if Word 97 (Word 8) or Word 2000 (Word 9) is running. If so, it reduces the level of the security warnings on Word so that you will receive no future warnings. In Word97, the virus disables the Tools/Macro menu commands, the Confirm Conversions option, the MS Word macro virus protection, and the Save Normal Template prompt. It "upconverts" to Word 2000 quite nicely, and there disables the Tools/Macro/Security menu.

Specifically, under Word 97 it blocks access to the Tools|Macro menu item, meaning you cannot check any macros. It also turns off the warnings for conversion, macro detection, and to save modifications to the NORMAL.DOT file. Under Word 2000 it blocks access to the menu item that allows you to raise your security level, and sets your macro virus detection to the lowest level, that is, none. (Since the access to the macro security menu item is blocked, I do not know how this feature can be reversed, other than programmatically or by reinstallation.)

After this, the virus checks for the HKEY_CURRENT_USER\Software\Microsoft\Office\Melissa? registry key with a value of "... by Kwyjibo". (The "kwyjibo" entry seems to be a

reference to the "Bart the Genius" episode of the "Simpsons" television program where this word was used to win a Scrabble match.)

If this is the first time you have been infected (and this "first time" business is slightly complicated), then the macro starts up Outlook, in the background, and sends itself as an attachment to the "top" 50 names in *each* of your address lists. (Melissa will *not* use Outlook Express.) Most people have only one (the default is "Contacts"), but if you have more than one then Outlook will send more than 50 copies of the message. Outlook also sorts address lists such that mailing lists are at the top of the list, so this can get a much wider dispersal than just fifty copies of the message/virus. There was also a mention on one message about MAPI and Exchange servers, which may give access to a very large number of mailing lists. From other reports, though, people who use Exchange mail server are being particularly hard hit. Then again, people who use Exchange are probably also standardized on Word and Outlook.

Some have suggested setting this registry key as a preventive measure, but note that it only prevents the mailout. It does not prevent infection. If you are infected, and the registry key is removed at a later date, then a mailout will be triggered the next time an infected document is read.

Once the messages have been sent, the virus sets the Melissa flag in the registry, and looks for it to check whether or not to send itself out on

subsequent infections. If the flag does not persist, then there will be subsequent mass mailings. Because the key is set in HKEY_CURRENT_USER, system administrators may have set permissions such that changes made are not saved, and thus the key will not persist. In addition, multiple users on the same machine will likely each trigger a separate mailout, and the probability of cross infection on a common machine is very high.

Since it is a macro virus, it will infect your NORMAL.DOT, and will infect all documents thereafter. The macro within NORMAL.DOT is "Document_Close()" so that any document that is worked on will be infected when it is closed. When a document is infected the macro inserted is "Document_Open()" so that the macro runs when the document is opened.

Note that *not* using Outlook does not protect you from the virus, it only means that the 50 copies will not be automatically sent out. If you use Word but not Outlook, you will still be infected, and may still send out infected documents on your own. The virus also will not invoke the mailout on Mac systems, but definitely can be stored and resent from Macs. At this time I do not have reliable information about whether it can reproduce on Macs (there is one report that it does), but the likelihood is that it can.

Vesselin Bontchev has noted that the virus never explicitly terminates the Outlook program. It is possible that multiple copies may be invoked, and may create memory problems. However, this has not been confirmed, and is

not probable given the "first time" flag that is set.

The message appears to come from the person just infected, of course, since it really is sent from that machine. This means that when you get an "infected" message it will probably appear to come from someone you know and deal with. The subject line is "Important Message From: [name of sender]" with the name taken from the registration settings in Word. The test of the body states "Here is that document you asked for ... don't show anyone else ;-)". Thus, the message is easily identifiable: that subject line, the very brief message, and an attached Word document (file with a .doc extension to the filename). If you receive a message of this form *DO NOT OPEN THE DOCUMENT WITH WORD!* If you do not have alternate means or competent virus assistance, the best recourse is to delete the message, and attachment, and to send a message to the sender alerting them to the fact that they are, very likely, infected. Please note all the specifics in this paragraph, and do not start a panic by sending warnings to everyone who sends you any message with an attachment.

However, please also note that, as with any Word macro virus, the source code travels with the infection, and it will be very easy to create modifications to Melissa. (The source code has already been posted to one Web site.) We will, no doubt very soon, start seeing many Melissa variants with different subjects and messages. There is already one similar Excel macro virus, called "Papa." The virus contains the text "Fred

Cohen" and "all.net," leading one rather ignorant reporter to assume that Fred was the author. Dr. Cohen was the first person to do formal research into viral programs.

There is a message that is displayed approximately one time in sixty. The exact trigger is if the current system time minute field matches the current system time day of the month field when the virus is run. In that case, you will "Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here." typed into your document. (This is another reference to the "Simpsons" episode referred to earlier.)

One rather important point: the document passed is the active document, not necessarily the original posted on alt.sex. So, for example, if I am infected, and prepare some confidential information for you in Word, and send you an attachment with the Word document, containing sensitive information that neither you nor I want made public (say, the fact that Bill Gates is a jerk for having designed the technology this way), and you read it in Word, and you have Outlook on your machine, then that document will be mailed out to the top 50 people in your address book.

Rather ironically, a clue to the identity of the perpetrator may have come from the identification number embedding scheme recently admitted by Microsoft as having been included with Office and Windows 98.

[Traced to an AOL user, apparently... PGN]

A number of fixes for mail servers and mail filtering systems have been devised very quickly. However, note that not all of these have fully tested or debugged. One version that I saw would trap most of the warning messages about Melissa.

Note that any Word document can be infected, and that an infected user may unintentionally send you an infected document. All Word documents, and indeed all Office files, should be checked for infection before you load them.

Information and antiviral updates (some URLs are wrapped):

<http://www.cert.org/advisories/CA-99-04-Melissa-Macro-Virus.html>

<http://www.ciac.org/ciac/bulletins/j-037.shtml>

<ftp://ftp.complex.is/pub/macrdef2.zip>

<http://www.complex.is/f-prot/f-prot.html>

<http://chkpt.zdnet.com/chkpt/hud0007500a/www.zdnet.com/zdnn/stories/>

news/0,4586,2233030,00.html

<http://www.zdnet.com/zdnn/special/melissavirus.html>

<http://www.symantec.com/techsupp/mailissa.html>

<http://www.antivirus.com/vinfo/security/sa032699.htm>

<http://www.avp.com/melissa/melissa.html>

<http://www.microsoft.com/security/bulletins/ms99-002.asp>

<http://www.sendmail.com/blockmelissa.html>

<ftp://ftp.rubyriver.com/pub/jhardin/antispam/procmail-security.html>

<http://www.innosoft.com/iii/pmdf/virus-word-emergency.html>

<http://www.sophos.com/downloads/ide/index.html#melissa>

<http://www.avertlabs.com/public/datafiles/valerts/vinfo/melissa.asp>

<http://www.pcworld.com/cgi-bin/pcwtoday?ID=10302>

http://www.internetnews.com/bus-news/article/0,1087,3_89011,00.html

<http://cnn.com/TECH/computing/9903/29/melissa.copycat.idg/>

<http://www.pcworld.com/cgi-bin/pcwtoday?ID=10308>

rslade@vcn.bc.ca rslade@sprint.ca robertslade@usa.net
pl@canada.com

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

✶ Melissa and monocultures

Nick Leverton <leveret@warren.demon.co.uk>

Wed, 31 Mar 99 13:54:52 GMT

The current outbreak of the Microsoft Word "Melissa" virus/worm is a graphical illustration of the RISKS of monoculture. Agriculturalists long ago discovered the problems of single strain crops, in that they provide an ideal habitat for an adapted pest or disease which can wipe them out.

With W97M/Melissa, the global e-mail network of at least one major international computer corporation with which I am familiar had to be disabled for 24 hours on Mon/Tue 1999-03-29 to 1999-03-30 to prevent the spread of Melissa-infected documents. (Melissa, for those fortunate enough not to have encountered it, is a Microsoft Word 97 macro virus, which also acts as a worm by reading 50 entries from a Microsoft address book and mailing itself out with subject "Important information from ...").

Ironically, and the point of this mail, sites within the corporation still running the older Unix/X.400 environment or the niche Unix/SMTP

environment

were unaffected, except that they were brought down too by the lack of connectivity from corporate mail gateways. A heterogeneous environment poses much greater barriers to the spread of this or any virus. Reliance on a single product or family of products, from a similar supplier, is a RISK that is familiar in the engineering and farming professions but needs to be better known in the computing ones.

Nick Leverton

[Lloyd Wood notes that Microsoft itself put a halt to all outgoing e-mail throughout the company on Friday to guard against propagation.]

Melissa and GUIDs

Ronan Waide <waider@scope.ie>
Tue, 30 Mar 1999 17:05:50 +0100 (IST)

Of course, conspiracy folks can enjoy the following course of events:

- 1 Presence of GUID in Microsoft-made documents revealed.
- 2 Melissa worm wreaks havok on the net.
- 3 Alleged author of worm tracked with GUIDs.

Let's wait for

- 4 Microsoft praised for having GUIDs in documents.

waider@scope.ie / Small Planet Ltd. / +353-1-8303455 / +353-1-8300888 (Fax)

✶ Melissa + meme = future disaster

Bear Giles <bear@coyotesong.com>

Sun, 28 Mar 1999 12:03:11 -0700 (MST)

While reading the press coverage about the Melissa e-mail virus/work, it occurred to me that a trivial change would make it *far* worse.

The problem was that Melissa advertised pornographic sites, so it was often brought to the attention of responsible parties who could recognize it was a virus and take appropriate measures. If it were a human virus, it would be something that sent people rushing to the doctor.

What if Melissa's message were something innocuous? What if it was a meme with a proven track record of being readily passed from person to person?

Make \$20,000 with only \$5!

Send your business card to a dying child seeking to get into the Guinness Book of World Records!

Send this message to 100 friends and get a free trip to Disney World from Bill Gates and Disney!

When people feel good, how many rush to the doctor to verify it isn't due to brain cancer? Of those who do, how many are taken seriously?

The most obvious effect of this change is that far fewer people would bring the message to the attention of their MIS department or ISP. Even hardened

security experts might let the message slide as just another scam or urban legend. Only the sheer volume of messages would indicate that something odd was occurring.

A less obvious effect of this change is even worse. Few people would forward an ad for pornographic sites on their own, but the aforementioned messages (and others) *are* forwarded. With changes. The current virus can be easily caught at the mail server by checking the subject line... but what if "helpful" individuals were personalizing it? Ditto the non-viral contents?

Even if it's technically possible to scan the contents of every mail document for an embedded macro virus, is it ethical? Such a filter would be invasive... and yet offer no guarantee that a copycat virus wouldn't get through. The real problem, after all, isn't in the virus itself, it's in an application for a *single* company defying all common sense and loading macros from e-mail. I think it's no coincidence that I haven't seen this virus... and I and my friends all run either Linux or MacOS.

Bear Giles <bgiles@coyotesong.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 20: Issue 27

Thursday 1 April 1999

Contents

- [RFC2550 - Y10K and Beyond](#)
- [Info on RISKS \(comp.risks\)](#)

✉ RFC2550 - Y10K and Beyond

Steve Glassman <steveg@pa.dec.com>
1 April 1999 00:00

Despite all of the hooplah about Y2K, computer programmers and protocol designers have not really learned from Y2K. Just because a problem seems far off, it should NOT be ignored. 30 years ago, the year 2000 seemed unimaginably far off and many protocols and programs were not designed to deal with it. Now, we see a similar problem on the horizon and we fear that most computer professionals are again looking the other way.

Starting with the year 10,000, years will have 5 digits. At least 16 RFCs and one ISO standard specify 4-digit years and countless programs

improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (1999). All Rights Reserved.

Abstract

As we approach the end of the millennium, much attention has been paid to the so-called "Y2K" problem. Nearly everyone now regrets the short-sightedness of the programmers of yore who wrote programs designed to fail in the year 2000. Unfortunately, the current fixes for Y2K lead inevitably to a crisis in the year 10,000 when the programs are again designed to fail.

This specification provides a solution to the "Y10K" problem which has also been called the "YAK" problem (hex) and the "YXK" problem (Roman numerals).

1. Introduction, Discussion, and Related Work

Many programs and standards contain, manipulate and maintain dates.

Comparing and sorting dates is a common activity. Many different formats and standards for dates have been developed and all have been found wanting.

Early date formats reserved only two digits to represent the year portion of a date. Programs that use this format make mistakes when dealing with dates after the year 2000. This is the so-called Y2K problem.

The most common fix for the Y2K problem has been to switch to 4-digit years. This fix covers roughly the next 8,000 years (until the year 9999) by which time, everyone seems convinced that all current

programs will have been retired. This is exactly the faulty logic and lazy programming practice that led to the current Y2K problem! Programmers and designers always assume that their code will eventually disappear, but history suggests that code and programs are often used well past their intended circumstances.

The 4-digit year leads directly to programs that will fail in the year 10,000. This proposal addresses the Y10K problem in a general way that covers the full range of date and time format issues.

1.1 Current approaches

A large number of approaches exist for formatting dates and times. All of them have limitations. The 2-digit year runs into trouble next year. The 4-digit year hits the wall in the year 10,000. A 16-bit year runs out in the year 65,536. A 32-bit counter for the number of seconds since 1970 [UNIX] wraps in 2038. A 32-bit counter for the number of milli-seconds since booting crashes a Windows (TM) PC in 49.7 days [Microsoft].

In this specification, we focus on the Y10K problems since they are most common and a large number of existing standards and protocols are susceptible to them (section 7). These standards, and new proposals on their way, will lead to a serious world-wide problem unless efforts are made now to correct the computing, government, and business communities.

Already, a small cottage industry is popping up to deal with the Y10K problem [YUCK]. We encourage these efforts and, in the coming years, this effort can only grow in size and importance.

1.2 A Fixed Format Y10K Fix

At the time of this writing, only one proposal [Wilborne] directly deals with the Y10K problem. In that proposal, dates are represented as decimal numbers with the dates compared numerically. The

proposed

format is simply YYYYMMDD - i.e. 5-digit years.

To allow numerical comparison of dates, this representation requires

a completely fixed representation for the date. There can be no optional fields, the date resolution is limited to the granularity of

one day, and this solution fails in the year 100,000 (Y100K).

1.2.2 Limitations of Numerical Comparison

While sufficient for the specific Y10K problem, this solution is limited. Even if extended for 6-digit years, it fails on 32-bit systems (and future 32-bit system emulators) after the date represented by the number 2147481231 (December 31, 214748) leading to

a Y214749 problem. Similarly, 64-bit and 128-bit systems also will

fail, although somewhat later (after December 31, 922,337,203,685,477

and December 31, 17,014,118,346,046,923,173,168,730,371,588,410 respectively).

1.2.3 Granularity Issues

The granularity problems of a fixed format date can be improved by extending the date format to include greater precision in the date.

However, since numerical comparison of dates requires a fixed representation date, an extended format can not provide sufficient resolution for all foreseeable needs.

For instance, if the precision were extended to the femto-second range the date format would become YYYYMMDDHHMMSSmmmuuunnnpppfff (year, month, day, hour, minute, second, milli-second, micro-second,

nano-second, pico-second, and femto-second). The additional 21 digits of this format limit the set of representable dates.

Compared

to 1.2.2, the 32-bit and 64-bit forms of the date are instantly exceeded, while the 128-bit version would be viable - expiring on December 31, 17,014,118,346,046.

1.2.3.1 Extrapolation of Future Granularity Issues

However, a simple extrapolation of Moore's law shows that even femto-second resolution will soon be inadequate. Projecting current

CPU clock speeds forward, a femto-second clock speed will be achieved

in only 30 years. And, by the year 10,000 the projected clock speed

of the Intel Pentium MMDCLXVI (TM) will be approximately 10^{1609} seconds.

This discussion clearly shows that any fixed-format, integer representation of a date is likely to be insufficiently precise for future uses.

1.2.3.2 Floating Point Is No Solution

The temptation to use floating point numbers to represent dates should be avoided. Like the longer fixed-format, integer representations of the date, floating point representations merely delay the inevitable time when their range is exceeded. In addition,

the well known problems of real numbers - rounding, denormalization, non-uniform distribution, etc. - just add to the problems of dealing with dates.

2 Structure of Y10K Solution

Any Y10K solution should have the following characteristics.

2.1 Compatibility

The format must be compatible with existing 4-digit date formats. Y2K compliant programs and standards must continue to work with Y10K

dates before the year 10,000. Y10K compliant programs can gradually

be developed over time and coexist with non-Y10K compliant programs.

2.2 Simplicity and Efficiency

Y10K dates must allow dates after 10,000 to be easily identified. Within a program, there must be a simple procedure for recognizing the Y10K dates and distinguishing them from legacy dates.

2.3 Lexical Sorting

Y10K dates must be sortable lexically based on their ASCII representation. The dates must not require specialized libraries or procedures.

2.4 Future Extensibility

Y10K dates must support arbitrary precision dates, and should support dates extending arbitrarily far into the future and past. Y10K dates from different eras and with different precisions must be directly comparable and sortable.

2.4.1 Environmental Considerations

The known universe has a finite past and future. The current age of the universe is estimated in [Zebu] as between 10^{10} and 2×10^{10} years. The death of the universe is estimated in [Nigel] to occur in 10^{11} - years and in [Drake] as occurring either in 10^{12} years for a closed universe (the big crunch) or 10^{14} years for an open universe (the heat death of the universe).

In any case, the prevailing belief is that the life of the universe (and thus the range of possible dates) is finite.

2.4.2 Transcending Environmental Considerations

However, we might get lucky. So, Y10K dates are able to represent any possible time without any limits to their range either in the past or future.

Y10K compliant programs MAY choose to limit the range of dates they

support to those consistent with the expected life of the universe.

Y10K compliant systems MUST accept Y10K dates from 10 ** 12 years in the past to 10 ** 20 years into the future. Y10K compliant systems SHOULD accept dates for at least 10 ** 29 years in the past and future.

3 Syntax Overview

The syntax of Y10K dates consists of simple, printable ASCII characters. The syntax and the characters are chosen to support a simple lexical sort order for dates represented in Y10K format.

All

Y10K dates MUST conform to these rules.

Every Y10K date MUST begin with a Y10K year. Following the year, there MAY be an arbitrary sequence of digits. The digits are interpreted as MMDDHHMMSSmmmmuunnnpppfff... (month, day, hour, minute, second, milli-second, micro-second, nano-second pico-second, femto-second, etc. - moving left to right in the date, digits always decrease in significance).

All dates and times MUST be relative to International Atomic Time (TAI) [NRAO].

When comparing dates, a date precedes every other date for which it is a prefix. So, the date "19990401000000" precedes the date "1999040100000000". In particular, dates with the format YYYYMMDD are interpreted to represent the exact instant that the day begins and precede any other date contained in that day.

3.1 Years 1 - 9999

The current 4-digit year syntax covers all years from 1000 - 9999. These years are represented as 4 decimal digits. Leading 0's MUST be added to the years before 1000 to bring the year to 4 digits. Files containing legacy pre-Y1K [Mike] dates will have to be converted.

732

consecutive 9's).

The formula for the number of digits in the year is, based on the two digit prefix is:

$$26 * (\text{ASCII}(\langle \text{prefix letter1} \rangle) - \text{ASCII}('A')) + \text{ASCII}(\langle \text{prefix letter2} \rangle) - \text{ASCII}('A') + 57$$

3.4.2.3 Years 10 ** 732 to 10 ** 18308

The next block of years has the number of digits given by three carets ("^^^") followed by three letters forming a three-digit, base

26 number. The number of digits in the year is given by the formula:

$$676 * (\text{ASCII}(\langle \text{prefix letter1} \rangle) - \text{ASCII}('A')) + 26 * (\text{ASCII}(\langle \text{prefix letter2} \rangle) - \text{ASCII}('A')) + \text{ASCII}(\langle \text{prefix letter3} \rangle) - \text{ASCII}('A') + 733$$

3.4.2.4 General Format for Y10K Dates

In general, if there is at least one letter in a Y10K year, the number of the digits in the year portion of the date is given by the formula:

$$\text{base26}(\text{fib}(n) \text{ letters}) + \text{y10k}(n)$$

Where "n" is the number of leading carets and the fig, base26 and y10k functions are defined with the following recurrence relations:

fib(n) is the standard Fibonacci sequence with:

$$\text{fib}(0) = 1$$

$$\text{fib}(1) = 1$$

$$\text{fib}(n+2) = \text{fib}(n) + \text{fib}(n+1)$$

base26(m letters) is the base 26 number represented by m letters

A-Z:

$$\text{base26}(\text{letter}) = \text{ASCII}(\langle \text{letter} \rangle) - \text{ASCII}('A')$$

$$\text{base26}(\text{string letter}) = 26 * \text{base26}(\text{string}) + \text{base26}(\text{letter})$$

y10k(n) is the necessary fudge factor to align the sequences

properly:

$$\text{y10k}(0) = 5$$

$$\text{y10k}(n+1) = 26 ** \text{fib}(n) + \text{y10k}(n)$$

If the year does not have at least one letter in the year, then the

number of digits in the year is:

4

This year format is space-efficient. The length of the prefix giving

number of digits in the year only grows logarithmically with the number of digits in the year. And, the number of carets preceding the prefix only grows logarithmically with the number of digits in the prefix.

3.5 B.C.E. (Before Common Era) Years

Now that we have a format for all of the years in the future, we'll take

on the "negative" years. A negative year is represented in "Y10K-complement" form. A Y10K-complement year is computed as follows:

- 1) Calculate the non-negative Y10K year string as in 3.4.2.4.
- 2) Replace all letters by their base 26 complement. I.E. A -> Z, B -> Y, ... Z -> A.
- 3) Replace all digits in the year portion of the date by their base 10 complement. I.E. 0 -> 9, 1 -> 8, ... 9 -> 0.
- 4) Replace carets by exclamation points ('!').
- 5) Four-digit years are pre-pended with a slash ('/')
- 6) Years that don't now begin with an exclamation point or slash are pre-pended with a star ('*'). (This rule covers the negative

5-

order)

for the time after the last instant of the A99999 and before the first instant of B100000:

```
A999991231250000
A999991232
A999992
A9999999999
A9999999999900000000000000000000
```

4 ABNF

The following ABNF [Crocker] gives the formal syntax for Y10K years.

The initial characters definitions are given in their lexical collation (ASCII) order.

```
exclamation = '!'
star         = '*'
slash       = '/'
digit       = 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9
letter      = A | B | C | D | E | F | G | H | I | J | K | L | M |
             N | O | P | Q | R | S | T | U | V | W | X | Y | Z
caret       = '^'
```

```
year        = [*(caret | exclamation) | star | slash ] [ *letter ]
             *digit
month       = 2digit
day         = 2digit
hour        = 2digit
minute      = 2digit
second      = 2digit
fraction    = *digit
date        = year [ month [ day [ hour [ minute [ second [ fraction
             ]]]]]]
```

5 Open Issues

There are a number date comparison problems that are beyond the scope of this specification.

1) Dates from different calendar systems can not be directly

compared. For instance, dates from the Aztec, Bhuddist, Jewish, Muslim, and Hittite calendars must be converted to a common calendar before comparisons are possible.

- 2) Future re-numberings of years are not covered. If, and when, a new "Year 0" occurs and comes into general use, old dates will have to be adjusted.
- 3) Continued existence of Earth-centric time periods (year, day, etc.) are problematical past the up-coming destruction of the solar system (5-10 billion years or so). The use of atomic-time helps some since leap seconds are no longer an issue.
- 4) Future standards and methods of synchronization for inter-planetary and inter-galactic time have not been agreed to.
- 5) Survivability of dates past the end of the universe is uncertain.

6 Affected Standards

A number of standards currently and RFCs use 4-digit years and are affected by this proposal:

rfc2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile
rfc2326: Real Time Streaming Protocol (RTSP)
rfc2311: ODETTE File Transfer Protocol
rfc2280: Routing Policy Specification Language (RPSL)
rfc2259: Simple Nomenclator Query Protocol (SNQP)
rfc2244: ACAP -- Application Configuration Access Protocol
rfc2167: Referral Whois (RWhois) Protocol V1.5
rfc2065: Domain Name System Security Extensions
rfc2060: Internet Message Access Protocol - Version 4rev1
rfc1922: Chinese Character Encoding for Internet Messages
rfc1912: Common DNS Operational and Configuration Errors
rfc1903: Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)
rfc1521: MIME (Multipurpose Internet Mail Extensions) Part One:

rfc1123: Requirements for Internet hosts - application and support

The following standards internally represent years as 16-bit numbers

(0..65536) and are affected by this proposal:

rfc2021: Remote Network Monitoring Management Information Base
Version 2 using SMIV2

rfc1514: Host Resources MIB

The following ISO standard is affected:

ISO8601: International Date Format

8 Security Considerations

Y10K dates will improve the security of all programs where they are

used. Many errors in programs have been tracked to overflow while parsing illegal input. Programs allocating fixed size storage for dates will exhibit errors when presented with larger dates. These errors can be exploited by wily hackers to compromise the security of

systems running these programs. Since Y10K dates are arbitrary length strings, there is no way to make them overflow.

In addition, positive Y10K dates are easy to compare and less error-

prone for humans. It is easier to compare the three projected end of

the universe dates - "H1000000000000", "I10000000000000" and "K1000000000000000" - by looking at the leading letter than by counting the 0's. This will reduce inadvertent errors by people. This advantage will become more noticeable when large dates are more common.

Unfortunately, negative Y10K dates are a bit more difficult to decipher. However, by comparing the current age of the universe to

its projected end, it is obvious that there will be many more positive dates than negative dates. And, while the number of negative dates for human history is currently greater than the number

of positive dates, the number of negative dates is fixed and the number of positive dates is unbounded.

9 Conclusion

It is not too early to aggressively pursue solutions for the Y10K problem. This specification presents a simple, elegant, and efficient solution to this problem.

10 References

- [Crocker] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.
- [Drake] Review for the Drake Equation
<http://www.umsl.edu/~bwilking/assign/drake.html>
- [Microsoft] SNMP SysUpTime Counter Resets After 49.7 Days
<http://support.microsoft.com/support/kb/articles/Q169/8/47.asp>
- [Mike] Y1K <http://lonestar.texas.net/~mdlvas/y1k.htm>
- [Nigel] Nigel's (en)lightening tour of Thermodynamics for Economists ;-)
<http://www.santafe.edu/~nigel/thermo-primer.html>
- [NRAO] Astronomical Times
<http://sadir.a.gb.nrao.edu/~rfisher/Ephemerides/times.html>
- [RFC] Here are all the online RFCs. Note: this is a LONG menu.
<http://info.internet.isi.edu/ls/in-notes/rfc/files>
- [UNIX] Year 2000 Issues <http://www.rdrop.com/users/caf/y2k.html>
- [Wilborne] PktCDateLig
<http://www3.gamewood.net/mew3/pilot/pocketc/pktcdate/index.html>
- [YUCK] Y10K Unlimited Consulting Knowledgebase
<http://www.loyd.net/y10k/index.html>
- [Zebu] The Search for H0
<http://zebu.uoregon.edu/1997/ph410/l6.html>

11 Authors' Addresses

Steve Glassman
Compaq Systems Research Center
130 Lytton Avenue
Palo Alto, CA 94301 USA

Phone: +1 650-853-2166
EMail: steveg@pa.dec.com

Mark Manasse
Compaq Systems Research Center
130 Lytton Avenue
Palo Alto, CA 94301 USA

Phone: +1 650-853-2221
EMail: msm@pa.dec.com

Jeff Mogul
Compaq Western Research Lab
250 University Avenue
Palo Alto, CA 94301 USA

Phone: +1 650-617-3300
EMail: mogul@pa.dec.com

12. Full Copyright Statement

Copyright (C) The Internet Society (1999). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other

Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an

"AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING

TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 28

Thursday 1 April 1999

Contents

- [Professor wants Y2K jokes banned on the Net](#)
[Edupage Editors](#)
- [Daylight Savings Time cutover](#)
[Dave Stringer-Calvert](#)
- [Y2K: Help for the Weary Programmer](#)
[Martin Minow](#)
- [IE5 Risk](#)
[Lorne Beaton](#)
- [The old Ethernet traffic jam in new form](#)
[Rob Slade](#)
- [More e-mail risks](#)
[Silas S. Brown](#)
- [Human input error on year causes \\$49-million error](#)
[Frank Carey](#)
- [Baby death due to software-controlled air bag deactivation?](#)
[Stefan Leue](#)
- [Hyperlinks, free accounts, and fraud](#)
[Mike Bell](#)
- [Melissa beyond denials of service](#)
[David Lesher](#)

- [Melissa macro virus author tracking](#)
[Joe Thompson](#)
 - [Y2K alert!](#)
[Rebecca Mercuri](#)
 - [Apple Y2K](#)
[Dave Stringer-Calvert](#)
 - [Re: Bringing Y2K fears to a new high -- or low](#)
[Gillian Richards](#)
 - [Re: Great moments in e-mail history?](#)
[Jerome H Saltzer](#)
[Tom Van Vleck](#)
[Jerome H Saltzer](#)
 - [Laughter causes loop with voice-recognition software](#)
[Don Mackie](#)
 - [Unusable backup power](#)
[Tim Kuehn](#)
 - ["kibibyte" is still ambiguous](#)
[D.V. Henkel-Wallace](#)
 - [Announcement - The Software Engineering Symposium '99](#)
[Carol Biesecker](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✉ Professor wants Y2K jokes banned on the Net

Edupage Editors <edupage@franklin.oit.unc.edu>

Thu, 01 Apr 1999 11:25:58 -0500

Insisting that "there's nothing funny about things that aren't funny,"

Professor Wiley T. Langweile of the Palo Alto (CA.)-based Institute of

Internet Reevaluation has written a searing letter to *The New York Times*

(1 Apr 1999) protesting that the American media are so bored with the Year

2000 problem that they're mentioning it only once in every 94.5 sentences

(by the professor's own hand-count). "Journalists are just not giving enough publicity to this impending crisis. They're either ignoring the problem entirely or making fun of it. Either way, they're acting unconscionably. Y2K irreverence needs to be banned, especially on the Internet." Dr. Langweile further charged in his letter that most reporters fail to include in their stories a detailed explanation of just what exactly the Y2K problem actually is and what it means to everyday people. "The low level of media competence on this issue is just tragic. Of course, there's Edupage. That's the big exception. Those Gehl and Douglas people really know how to get to the point of a story, without wasting words. They're the only ones I can think of who've successfully explained Y2K in terms of the big hand and the little hand. I say God bless them." (Edupage, 1 Apr 1999)

[Note to nonGermanophiles: "Langweile" relates to Boredom, not Coyotes. Definitely not the case here. PGN]

⚡ Daylight Savings Time cutover

Dave Stringer-Calvert <dave_sc@csl.sri.com>
Thu, 01 Apr 1999 09:43:11 -0800

Please note the following!

Washington DC (Reuters, 1 April 1999), Roger Tempus, News Staff

In a sweeping move to alleviate the problems generated by the switch to daylight savings time early on Sunday morning, Congress voted today to

move the switch to Monday.

There has been a long history of confusion surrounding the switch to daylight savings time, and in a landslide vote this morning members of the house made a decisive move to make daylight savings a more attractive option. This was given wide support amongst the religious groups, concerned that people would be confused as to the timings of church services this Easter Sunday.

Congresswoman April Jester (R, CA) confirmed the news this morning and announced that the changeover will now take place at 10am on Monday morning.

In a dramatic turnabout, the state of Arizona decided that in light of this decision they too will adopt daylight savings time for 1999.

Wall Street reacted angrily to the news, claiming that the lost hour of trading may drop the country back into recession. President Clinton is expected to sign the order confirming the change this afternoon, claiming that bedtime is just as, if not more, important than work time.

✶ Y2K: Help for the Weary Programmer

Martin Minow <minow@apple.com>

Wed, 31 Mar 1999 23:02:39 -0800

While reading several articles on the Y2K problem in the 1 April 1999 issue of [RISKS-20-26](#), I noticed that none addressed the actual problem facing

working programmers: there isn't enough time to finish the job before
December 31. As we all know from The Mythical Man Month, we can't add more
people to the project: the project will just take longer. What we need is
another month.

I propose Caligua. To honor Roman tradition, this would be added after
August. This extra month should give us enough time to fix -- and test --
our changes. While it will cause minor disruption to calendar makers and
astronomers, they, along with all other citizens, will reap the rewards when
the airplanes keep flying on 1 Jan 2000.

And, if we need more time, we can always declare a Saturnalia.

Martin Minow, minow@pobox.com

[Martin drives a Saturnalias for Caligula. PGN]

⚡ IE5 Risk

Lorne Beaton <lbeaton@MNSi.Net>

Thu, 25 Mar 1999 00:19:49 -0500

Browsing the Web this evening (Thursday, March 24, 1999) using the new IE5 under Windows 98, I click a Favourite to load a well-known tech news site (<http://www.slashdot.org/>), then, with the site still loading, immediately press Control-N to open a new window so that I can load another site as well. A moment later, I'm a bit puzzled to notice that Slashdot hasn't been

updated since Sunday the 21st. This is particularly puzzling since I had checked it earlier that day, using my work account, and it was up to date.

My confusion is relieved a moment later, when I notice the site loading up in the background window (the one that was already open). I have been looking at the newly-opened window, which appears to have inherited one piece of state from the previous one (i.e., the URL being displayed) but not another (i.e., the crucially important fact that the site needs to be updated, not just redisplayed from the cache).

Contrast this with the behaviour of other web browsers (e.g., Netscape Communicator 4.51). In a desultory test, Communicator acted correctly (i.e., displayed up-to-date information in a new client window, even as the previous window was still reloading the site). This was done with Communicator set to load "Last page visited" when opening new client windows. It appears that Communicator 4.51 checks this setting each time a new client window is opened, whereas IE5 checks this setting only once, when launched. There also appears to be no way to change this behaviour.

Possible risk (which I have not noticed in previous versions of IE, although it may be present there as well) is that a less-observant or more naive user might assume the outdated information is actually up-to-date and correct.

Lorne Beaton <lbeaton@mnsi.net>

⚡ The old Ethernet traffic jam in new form

Rob Slade <rslade@sprint.ca>

Tue, 23 Mar 1999 14:35:48 -0800

I am currently trying to download something from Microsoft--for the eleventh and twelfth time in the past five days.

The problem, of course, is probably the recent announcement of IE5.

Everybody and his or her dog is trying to download the latest and buggiest browser. (Bob Frankston's problem with his bank is only one of many: Visual Studio 6 and Eudora Pro both have problems with it, and then there is the AutoComplete function ...)

However, I am inescapably reminded of the old problem with Ethernet, and Carrier Sense Multiple Access with Collision Detect. As traffic rises collisions grow more common. Therefore, there are more retries on the net, and therefore traffic rises and ... (Anyone who has to commute over a busy bridge knows why network traffic analysis is called "traffic" analysis.) Same thing is probably happening here. More people are trying to download the files from Microsoft. Therefore, more downloads fail, therefore more people try again, therefore ...

Yes, I'm contributing to the problem: I'm running two separate downloads in the hopes that one will finally succeed. Probably a lot of net-savvy people are doing the same thing, or better (worse?)

Completely beside the point, the program I am trying to download is the new version of MediaPlayer. On Friday it was a 4.8 meg file. Today the same file is 3.4 meg. One of the never-to-be-known mysteries of the net, I guess ...

rslade@vcn.bc.ca rslade@sprint.ca robertslade@usa.net
pl@canada.com

⚡ More e-mail risks

"Silas S. Brown" <ssb22@cam.ac.uk>

Mon, 22 Mar 1999 08:11:20 +0000

> Once again we are reminded of the incredible variety of risks of e-mail.

Here's a really strange one: Ever heard of PostPet? It's a Japanese computer game that's also an e-mail client. Besides limited capability to deal with normal mail, you can send your "pet" with the message to another PostPet user. Your pet gets sent as an attachment and returned immediately upon delivery with updated status (depending on how your friend treats your pet etc); there is a timeout. (It gets returned in a "Secret Diary" message supposedly written by the pet; the language of this diary depends on that of the destination client.) Pet mail also causes the addition of the sender to the recipient's list of friends.

Risks:

1. If too many people use this thing, we may get spamming incidents in

which the spammer adds a PostPet attachment to the spam, thus ensuring a personalised delivery, a guaranteed response from valid addresses and an addition to people's personal contact lists.

2. The file format of the attachment can be reverse-engineered, and a response generated artificially, for any social purpose whatsoever. In fact, once someone has sent you their pet, you can keep its ID for use later - all you have to do at any time is send a message with a custom status and arrange for it to arrive while the pet is "out".

3. There is no way of viewing full headers, and hence if someone is abused etc they can't report it. (Many other things can't be done, too.)

4. Games aren't really meant to live in the application world. If they ported it to Unix, it could consume vast amounts of CPU on a shared system and equally vast amounts of network bandwidth updating the display.

5. The buttons for "send pet" and "send normal e-mail" are far too close.

6. This is no way to introduce e-mail to people new to computers, and yet it is (apparently) being used for that in Japan. This could lead to people not learning things properly. The PostPet documentation is full of metaphors that don't really tell you what's going on.

7. It generally increases the amount of pointless e-mail and wasted time.

-- Silas S Brown, St John's College Cambridge UK <http://epona.>

ucam.org/~ssb22/

⚡ Human input error on year causes \$49-million error

Frank Carey <carey@voicenet.com>

Mon, 22 Mar 1999 09:45:53 -0500

On 21 Mar 1999, 180,000 families in New Jersey receiving food-stamps took advantage of an error by which their April credits were enabled 10 days early. In the 15 hours until the problem was discovered and fixed, the word spread rapidly and shoppers went on a feeding frenzy. Many stores ran out of staples (food, not metallic). A state employee was preparing for the 1 Apr 1999 crediting of food-stamp accounts; discovering that performance was dragging seriously, he off-loaded the processing onto the backup mainframe, and then moved the resulting files back to the main system. Initial blame was placed on a recent Y2K upgrade, but later reports observed that he had input "199" instead of "1999" in making the cutover, and the program coerced a zero on the end to make the year "1990". So, perhaps the problem was indirectly Y2K-related after all. [Source: *The New York Times* 22 Mar 1999, p. B1; *Newark Star Ledger* 22 Mar 1999, p. 13, with revisions to absolve Y2K two days later, *NYT* 24 Mar, B5. PGN-ed, starkly]

⚡ Baby death due to software-controlled air bag deactivation?

Stefan Leue <sleue@fee.uwaterloo.ca>

Mon, 29 Mar 1999 23:54:00 -0500 (EST)

Under the headline "Vom Retter erschlagen" ('Slain by the Savior') the German weekly "Der Spiegel" (<http://www.spiegel.de>) reports on page 226 in its issue 12/1999 on the analysis of an accident in which a baby sitting in a rear facing car seat mounted to the front seat in a Volkswagen Golf was killed by the impact of the deploying air bag in an oncoming traffic collision. The car owners and parents of the killed baby had previously had the air bag disabled in a certified garage.

The wreck of the car is currently sealed by the public prosecutor's office and inaccessible to Volkswagen and the manufacturer of the air bag electronics, Siemens. Volkswagen maintains that the deployment of the air bag may either have been caused by a voltage surge in the car's electronic system resulting from the impact on the battery, or by electrostatic discharges.

Experts from the Technical University of Munich, working for the public prosecutor's office, consider these explanations implausible and target a systems engineering fault as a more likely causal factor. Deactivation of the airbag in a Golf is a software-controlled function, as opposed to other manufacturers who physically disconnect the air bag from the board electronics for deactivation. As physical circumstances in a car (temperature variations, moisture, vibrations) form a fairly hostile

environment for the air bag control hardware, the software system running inside the control performs ongoing self checks using checksum algorithms. If an error has been detected, the current software settings, including the data responsible for the deactivation, will be replaced by backup software read out of a read-only memory. The backup software, however, only knows a simple set of rules, namely that all air bags in the car will be deployed upon impact. Evidently, the backup software is unaware of a previous software-controlled deactivation.

Stefan Leue

✶ Hyperlinks, free accounts, and fraud

Mike Bell <mbell@albionresearch.com>

Mon, 22 Mar 1999 09:28:18 -0500

SPAM-L this week contained a description of interesting method being used to obtain credit-card numbers.

1. Grab e-mail addresses of AOL users in chat rooms.
2. Mail them a forged message from AOL asking them to click on a hyperlink to verify their billing details. "Click here" takes them to a forged AOL page on a free web service asking for exact credit card details, passwords, etc.
3. If they fill out the form, it is POSTed to an innocent cgi script on another site which accepts a hidden argument specifying an e-mail address where the credit card information will be mailed to.
4. Finally the cgi script redirects the user to a third throw-away site

("Thank you for changing your account details").

5. The perpetrator can now pick up a list of credit card numbers from the free e-mail account from anywhere in the world.

The basic risk here is an old one: clicking on a hyperlink may not always take you where you think. In addition the use of free anonymous e-mail accounts and web pages makes it far easier for the criminal to avoid a simple paper trail.

-- Mike --

✶ Melissa beyond denials of service

David Leshar <wb8foz@nrk.com>

Thu, 1 Apr 1999 13:37:47 -0500 (EST)

One thing only a fraction of the popular press coverage has touched upon is that: while spreading itself around the world, Melissa also appears to send the document the victim is dealing with at the time as well.

THAT may have consequences that last far past the Denial of Service logjam. If the file in Word was confidential and Melissa leaks [..you name it..] out....

This might draw some attention to other Word problems; such as its propensity to send along both deleted text as well as that from other document windows. It does not show when rendered by Word, but it's still there....

(A friend at a Fortune 500 communications company recently was sent a doc whose distribution was limited to 5 or 6 people. He used the Unix tool 'catdoc' to read it on his workstation & discovered most of an innocuous 2nd doc also in the file. "Suppose it had been the other way around?" he remarked.)

Such covert channels have always been a concern some people paid serious attention to [witness IntelLink's physically separate networks for U, S, and TS/SCI; and the recent release of AES material via printer-->scanner-->PDF route]; I hope more people will now do likewise...

🔥 Melissa macro virus author tracking

Joe Thompson <fbi.gov@orion-com.com>
Thu, 01 Apr 1999 01:25:02 -0500

As it turns out, the GUID is **not** a reliable identifier of the author for the Melissa virus:

<http://www.zdnet.com/zdnn/stories/news/0,4586,2234018,00.html>

Synopsis: If a Word document is passed to another person, modified, and saved, the original GUID is preserved even though none of the actual content may still be extant. In this case, the GUID in question has been discovered in works from other authors. The person currently under the most suspicion (known as VicodinES) says that the virus code in his document

that has the same GUID as Melissa (a macro virus named PSD2000.DOC) is actually based on earlier virus code from another author (known as ALT-F11); indeed, the GUID on that earlier work **also** matches Melissa. So does the GUID on other work by ALT-F11, while work that VicodinES claims is original with him does **not** have the Melissa GUID. **Anyone** could have written Melissa and made VicodinES, or any other Word user they want, appear to be the culprit.

Here we see the inherent RISK of relying on a non-unique identifier; in this case, the fact that the ID is inherited poses additional risks of misidentification. -- Joe

Joe Thompson <http://kensey.home.mindspring.com/> fbi.gov@orion-com.com

[Even if they are unique, such IDs may be easily forged. Once again, the use of digital evidence is tricky. PGN]

⚡ Y2K alert!

Rebecca Mercuri <mercuri@gradient.cis.upenn.edu>
Thu, 18 Mar 1999 00:20:00 -0500 (EST)

--- Forwarded mail from a colleague at Disney ---
FINALLY! A Programmers Drinking Song! Woo! Hoo!

PROGRAMMERS DRINKING SONG:

99 little bugs in the code,
99 bugs in the code,
fix one bug, compile it again,

```
101 little bugs in the code.  
101 little bugs in the code.....  
(Repeat until BUGS = 0)
```

[I think it's appropriate, given the rash of "buggy" animations these days.

Rebecca.] [It's nice that Y2K is also brewing lyrics. PGN]

🔥 Apple Y2K

Dave Stringer-Calvert <dave_sc@csl.sri.com>

Wed, 17 Mar 1999 22:23:46 -0800

This is cute:

```
>           "We may not get everything right,  
>           but at least we knew the century was going to end."  
> -- Apple Computer, HAL 9000 ad for Macintosh Y2K compliance
```

🔥 Re: Bringing Y2K fears to a new high -- or low (Gerlek, [RISKS-20.24](#))

"Gillian Richards (02) 4780 3513" <gillian.richards@tafensw.edu.au>

Wed, 17 Mar 1999 13:47:42 +1100

```
> [...] We don't want people going and buying  
> generators when they should be out buying jeans."
```

There's another *hidden* problem. In Australia, the most common brand of

zippers (zip-fasteners) used on manufactured clothing is YKK.

I have no idea what sort of compliancy tests to run on my zippers, and, wishing to take *no* risks of the "system" being down at the

wrong time,
will be wearing either buttons or elastic on 31 December 1999.

Gillian Richards, Computer Systems Officer <gillian.
richards@tafensw.edu.au>
Wenworth Falls TAFE Campus, NSW Australia

✉ Re: Great moments in e-mail history? (Neugent, [RISKS-2.25](#))

Jerome H Saltzer <Saltzer@MIT.EDU>
Mon, 22 Mar 1999 23:06:17 -0500

Part of the problem is that the definition of e-mail is a bit fuzzy. If you define it to mean any mail-like electronic message, then you can trace it back to 1851, when the New York and Mississippi Valley Printing Telegraph Company (predecessor of Western Union) began sending telegrams. The AUTODIN messaging system may belong in that family tree.

If you mean mail-like messages between computer users, then CTSS certainly had a mail command that may be a candidate for first. If Corby [Corbato] searches his attic, he might be able to find a date earlier than the circa January 1965 PSN you identified. A survey of the other time-sharing systems of the time would probably turn up some other mail programs.

But that didn't go between machines. If e-mail means that two computers have to be involved, then Kleinrock may well have sent the first piece of e-mail that crossed the net. I don't recall that we ever had mail moving between the two CTSS machines (MAC and Computation Center) at

MIT.

Jerry

✉ **Re: Great moments in e-mail history? (Neugent, [RISKS-20.25](#))**

Tom Van Vleck <thvv@multicians.org>

Mon, 22 Mar 1999 23:01:57 -0800

AUTODIN probably counts as one of the "first" e-mail systems. As I remember, there was a BBN project called "Mercury" that was also working on electronic mail. Noel Morris and I knew that both of these existed when we wrote CTSS MAIL, but were not sure whether Mercury was ever deployed.

PSN 40 _proposed_ a MAIL command. As I remember, Noel and I, junior energetic programmers, offered to do it while others were busy with Multics design, and were given permission. When I visited Roger Roach about 8 years ago, he still had the CTSS source, and I looked at the source of MAIL, and it was my code. It had Dick Mills's, Bill Bierstadt's, and my programmer numbers baked into the code. We, and M1416 * could send messages to all users. (See my story, quoted in _Wired_, about the first spam, sent by Peter Bos. Remember that? He abused his system programmer privilege to send a message beginning THERE IS NO WAY TO PEACE. PEACE IS THE WAY. When I remonstrated, he said, "But this is *important.* Wired got my name wrong. Peter Bos and Noel are both gone.)

>... If e-mail means that two computers have to be involved, ...

That definition would of course depend on the meaning of "computer." Would Tandem's multi-node, multi-CPU, single-system-image MAIL qualify? In some senses that system was a 645 with very long buses. Was it one computer or many? Was the 645?

✶ Re: Great moments in e-mail history? (Van Vleck, [RISKS-20.28](#))

Jerome H Saltzer <Saltzer@MIT.EDU>

Tue, 23 Mar 1999 09:32:10 -0500

Here is another try at imposing categories and milestones on what looks more and more like continuous evolution:

1. First mail-like communication by electronic means (telegrams): 1851, Mississippi Valley Printing Telegraph Company.
2. First interposition of computers in handling mail-like communication: perhaps 1957, TELEX, and probably also some predecessors of AUTODIN.
3. First mail-like communication within a system used for general-purpose computing: early 1960's, Van Vleck & Morris on CTSS or perhaps BBN Project Mercury.
4. First mail-like communication between two computers operated by different administrative entities: late 1960's, perhaps Kleinrock's anecdote, but it needs some more research.

Lenny Kleinrock can probably claim without fear of contradiction that he sent the first e-mail over the ARPANET, because he was standing at one end of the first ARPANET link that was installed. The fact that Kleinrock's anecdote is dated at practically the instant of that installation is pretty compelling evidence that e-mail was already well-known and operating within individual time-sharing systems.

Jerry

⚡ Laughter causes loop with voice-recognition software

Don Mackie <donald@iconz.co.nz>

Sat, 13 Mar 99 16:41:39 +1300

My son has dyslexia. To help him deal with life, he has some voice-recognition software on his PC. In the early stages of training he found that odd noises, such as laughter, were interpreted by the computer and, at best, produced long strings of random words. Having a normal teenager's sense of humour he found these funny, laughed some more and so on. When his giggles subsided he had to utter the command "delete last four pages". I now recognise the signs of mirth in his e-mails.

Even funnier is getting the computer to read back the laughter passages.

✦ Unusable backup power (Re: Weingart, [RISKS-20.24](#))

Tim Kuehn <timk@tdkcs.waterloo.on.ca>

Mon, 22 Mar 1999 10:01:40 -0500

> ... It's not enough to have a backup system in place...you
need to make
> sure it will work when needed.

... and that if it's there you're able to or allowed to connect
to it.

A colleague maintains a number of Internet Web servers as a
commercial
venture. Friday he found out that the building that houses
these servers
was going to be disconnected from the power mains for 8 hours
starting at
midnight Saturday in order to conduct an annual power audit.

The company he was renting space from didn't have enough
capacity in their
battery backup systems to run his equipment, but would have the
system
upgraded "next month." The room is sealed, so putting in a small
internal-combustion driven generator was out. There is a diesel-
powered grid
in place, but it only generates 48V DC used by a number of telco
switches in
the room. And trying to find a sufficiently sized 48VDC to
110VAC inverter
for rent was an exercise in futility. A number of vendors were
more than
willing to sell him one of these ~\$4K devices however.

The risk here is that even if backup power's available, you may
not be able
or allowed to use it.

Tim Kuehn

⚡ "kibibyte" is still ambiguous (Re: Edupage, [RISKS-20.25](#))

"D.V. Henkel-Wallace" <gumby@zembu.com>

Mon, 29 Mar 1999 18:30:56 -0800

The new term "kibibyte" will more accurately describe the number of bytes in a kilobyte -- rather than being 1,000, as could be inferred by the prefix "kilo," a kilobyte actually has 1,024 (2 to the 10th power) bytes.

Has the 8-bit usage of the term "byte" been internationally standardized?

Or is "kibibyte" still ambiguous (for Multics and PDP-10 hackers at least)?

"Kibiocets" anyone? Sounds like a cat food.

David Henkel-Wallace, Zembu Labs

⚡ Announcement - The Software Engineering Symposium '99

Carol Biesecker <cb@SEI.CMU.EDU>

27 Mar 1999 22:08:30 GMT

The Software Engineering Symposium '99

Theme: Improving the State of Software Engineering:
Principles, Practices, and Projections

August 30--September 2, 1999

David L. Lawrence Convention Center
Pittsburgh, Pennsylvania

Early Bird Registration: July 28, 1999

For the most up-to-date information, bookmark our Web site at

<http://www.sei.cmu.edu/products/events/symp/>

or contact

Symposium '99 Conference Coordinator

Software Engineering Institute

Carnegie Mellon University

Pittsburgh, PA 15213-3890

Phone: 412 / 268-3007

FAX: 412 / 268-5556

E-mail: symposium@sei.cmu.edu



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 29

Friday 2 April 1999

Contents

- [Attack of the Tuxissa Virus](#)
[Anonymous](#)
- [Computer crash creates nonpersons in Zurich](#)
[Bruce Walker](#)
- [tcpd warning](#)
[Kragen Sitaker](#)
- [Saving files on shared computers](#)
[Bertrand Meyer](#)
- [Self-opening car windows ...](#)
[Jeremy Folkes](#)
- [Swedish telephone outage](#)
[Danny Kohn](#)
- [Electricity over Internet](#)
[Lionel Cons](#)
- [In the summertime, when your VCR screws up](#)
[Michael Bacon](#)
- [Brain-dead PacBell automated payment promise system](#)
[Michael D. Crawford](#)
- [Re: Unusable backup power](#)
[Terry Harris](#)

- [Origins of PC / Mac Virus Vulnerability](#)
[Mich Kabay](#)
 - [Re: More e-mail risks](#)
[Michael H Buselli](#)
 - [Re: Apple Y2K](#)
[Art Delano](#)
 - [REVIEW: "Information Warfare and Security", Dorothy Denning](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Attack of the Tuxissa Virus

Anonymous <nobody@REPLAY.COM>
Tue, 30 Mar 1999 05:31:34 +0200

[Contributed belatedly by several RISKS readers. TNX. Sorry we could not have included it in one of YESTERDAY'S three issues. PGN]

LART* Advisory LA-99.01.Tuxissa
Original issue date: Apr. 0a, 1999
Last revised: --

Topic: Attack of the Tuxissa Virus

This advisory is intended primarily for network administrators responsible for user configuration and maintenance.

Attack of the Tuxissa Virus, March 29, 1999

What started out as a prank posting to comp.os.linux.advocacy yesterday has turned into one of the most significant viruses in computing history. The creator of the virus, who goes by the moniker "Anonymous Longhair", modified the well-known Melissa [1] virus to download and install Linux on infected

machines.

"It's a work of art," one Linux advocate told Humorix after he looked through the Tuxissa virus source code. "This virus goes well beyond the feeble troublemaking of Melissa." The advocate enumerated some of the tasks the virus performs in the background while the user is blissfully playing Solitaire.

Once the virus is activated, it first works on propagating itself. It has a built-in e-mail harvesting module that downloads all the pages referenced in the user's Internet Explorer bookmarks and scans them for e-mail addresses. Using Outlook, the virus sends a copy of itself to every e-mail address it comes across.

After it has successfully reproduced, the virus begins the tricky process of upgrading the system to Linux. First, the virus modifies AUTOEXEC.BAT so that the virus will be re-activated if the system crashes or is shut down while the upgrade is in process. Second, the virus downloads a stripped-down Slackware distribution, using a lengthy list of mirror sites to prevent the virus from overloading any one server.

Then the virus configures a UMSDOS filesystem to install Linux on. Since this filesystem resides on a FAT partition, there is no need to re-partition the hard drive, one of the few actions that the Word macro language doesn't allow.

Next, the virus uncompresses the downloaded files into the new

Linux

filesystem. The virus then permanently deletes all copies of the Windows Registry, virtually preventing the user from booting into Windows without a re-install. After modifying the boot sector, the virus terminates its own life by rebooting the system. The computer boots into the Slackware setup program, which automatically finishes the installation of Linux. Finally, the dazed user is presented with the Linux login prompt and the text, "Welcome to Linux. You'll never want to use Windows again. Type 'root' to begin..."

The whole process take about two hours, assuming the user has a decent Internet connection. Since the virus runs invisibly in the background, the user has no chance to stop it until it's too late.

The e-mail message that the virus is attached to has the subject "Important Message About Windows Security". The text of the body says, "I want to let you know about some security problems I've uncovered in Windows 95/98/NT, Office 95/97, and Outlook. It's critically important that you protect your system against these attacks. Visit these sites for more information..."

The rest of the message contains 42 links to sites about Linux and free software.

Slashdot is one of those links. "That could spell trouble," one Slashdot expert told Humorix. "Slashdot could fall victim to the new 'Macro Virus Effect' if this virus continues to propagate at its present exponential

growth rate. Red Hat's portal site, another site present on the virus' links list, seems to be quite sluggish right now..."

Details on how the virus started are a bit sketchy. The "Anonymous Longhair" who created it only posted it to Usenet as an early April Fool's gag, a demonstration of how easy it would be to mount a "Linux revolution". Some other Usenet reader is responsible for actually spreading the virus into the wild. One observer speculated, "I imagine the virus was first sent to the addresses of several well-known spammers. The virus probably latched on to the spammer's e-mail lists and began propagating at a fantastic rate. With no boundary to its growth, this thing could wind up infecting every single Net-connected Wintel box in the world. Wouldn't that be a shame!"

Linus Torvalds, who just left for a two week vacation, was unavailable for comment at press time. We have a strong feeling that his vacation will be cut short very soon...

[1] <http://linuxtoday.com/stories/4463.html>

James S. Baughn <http://i-want-a-website.com/about-linux/>

[For those of you not familiar with the imagery, think about what erect short-legged flightless aquatic-bird operating-system symbol seems to be wearing a tux. But then don't ask about who the Mel in Melissa is. PGN]

⚡ Computer crash creates nonpersons in Zurich

"Walker, Bruce" <bwalker@logicon.com>

Thu, 1 Apr 1999 10:47:57 -0800

I found this one while surfing the web

One side effect of the year 2000 problem; crash in central computer

On Wednesday afternoon, 31 Mar 1999, the central computer of the Zurich city administration crashed due to a mistake by two officials who were working on the reprogramming the cantonal and city information systems for Y2K. After rebooting the computer, they found that important files were missing -- including those containing data on the citizens of Zurich, many of whom may have become ``officially lost'', according to a city councillor. [Source: *Zurich Tages-Anzeiger*, 1 April 1999, PGN-ed from the German and from Bruce's translation]

My comment is: where were the backup tapes?

Bruce Walker 1406 Stonewood Ct. San Pedro, Calif. 90732

⚡ tcpd warning

Kragen Sitaker <kragen@pobox.com>

Fri, 2 Apr 1999 17:32:51 -0500 (EST)

The problem with tcpd that's being discussed on BUGTRAQ -- that a backslash at the end of a comment line has a meaning different from the one a

particular user was expecting -- illustrates a larger problem.

Simple, predictable user interfaces are essential to security. If you must direct a program to take some action, and you cannot tell whether the action you have directed it to take is dangerous or not, then your system is insecure, because there is a significant chance you will accidentally do something dangerous.

You don't want DWIM in your hosts.allow and hosts.deny files. You don't want confusingly-difficult syntax, either.

In general, this is an argument against using computers to safeguard security, because computers are hard to predict. (Much harder, for example, than deadbolts.) But there are cases in which you have to do this; in these cases, it is imperative to use software that is as transparent as possible, so you can have a high degree of assurance that it will do the right thing.

qmail's config files are good in this way: very, very simple. Very hard to get surprising behavior -- at least, surprising to me. It is quite likely that new Unix users would be surprised by it frequently, and I don't know any way around that.

Usability is essential to security.

<kragen@pobox.com> Kragen Sitaker <<http://www.pobox.com/~kragen/>>

⚡ Saving files on shared computers

<Bertrand.Meyer@eiffel.com>

Tue, 30 Mar 1999 20:06:01 -0800

Mail from: Bertrand Meyer (Interactive Software Engineering, Santa Barbara)

Recently I used a public access computer graciously provided by HP in an American Airlines Admiral's Club. Although a long-time RISKS reader, I couldn't believe my eyes when looking under "Documents" in the Windows taskbar. Previous users had stored all kinds of Word documents, including one entitled "Confidential Settlement Terms", personal correspondence etc.

The service is extremely useful. I would be sorry if pointing out its risks incited its providers to restrict it. Still, people who offer such shared services should think of sticking on the computer a note of the form "When you are done, remember not to leave behind any personal file".

-- Bertrand Meyer, ISE, Santa Barbara
Bertrand.Meyer@eiffel.com, <http://eiffel.com>

⚡ Self-opening car windows ...

Jeremy Folkes <jf@jeremyf.cix.co.uk>

Sun, 28 Mar 1999 0:20 +0000 (GMT Standard Time)

A few weeks ago I took delivery of a shiny new Ford Galaxy - a 7 seater "people-mover". About two weeks later I came out of the house in the

morning to find both front windows open - although I was convinced that I'd shut it all up the night before. My wife didn't really believe me, but then it happened to her - she parked it up with the windows closed, and when she returned to the car, the windows were opened. She took it to the garage, they didn't really believe her, until it happened to them....

In the good old days when windows were opened by turning a handle, they tended to stay in the position you left them. Now with electronics taking over, I had a car which would randomly open its windows when left alone. Luckily, nothing was stolen, but had I have been parked in a different place, it could have been more serious - or at the least if it had been raining I could have come back to a very wet car.

The Risks. Technology may be convenient, but it brings all sorts of new failure modes that we probably never envisaged. The cleverer it gets, the more opportunity for things to go wrong....

Jeremy

Swedish telephone outage

"Danny Kohn" <danny.kohn@systematik.se>

Thu, 25 Mar 1999 14:13:31 +0100

After a number of ISDN outages last year and some this year in the country, our nationally owned telco Telia had two big outages in the capital of Stockholm. It happened the first time Monday 15 Mar 1999, when

millions of
phone lines including the police headquarters' PBX were unusable
for 8
hours! The outage was repeated exactly a week later between
10:25am and
11:05am, when incoming calls to the police PBX and to another
250 business
PBXs where blocked.

The second outage is explained as an intermittent error that
disturbed the
communication between PBXs and the telco equipment. In addition
the
software that would localize the problem had a bug so that the
error would
not display.

The police management said that they trust Telia that this
problem is now
fixed.

Comming to mind is that telco exchanges are often purchased in
international
competition. A telco operator can not see through the
software. But given
the complexity neither can the producer -- we might not have
bugs if they
did. So, if a intruder paid by some nearby country wanted to,
he could
program some code "detonating" as a part of war attack.

Danny Kohn Systematik Consulting AB <http://www.systematik.se> +46
(0)708 140300

Electricity over Internet

Lionel Cons <lionel.cons@cern.ch>
Tue, 30 Mar 1999 14:47:17 +0200 (METDST)

There's no doubt that the Internet relies on electricity, it seems that some may have electricity relying on the Internet:

In Latest E-Commerce Play, Venture Sells Electricity Online - Internet

World 3/22/99

<<http://www.internetworld.com/print/current/news/19990322-latest.html>>

This is a nice chicken and egg problem: which one will fail first?

Lionel Cons <http://home.cern.ch/~cons>

CERN <http://www.cern.ch>

⚡ In the summertime, when your VCR screws up

Michael Bacon <streaky_Bacon@email.msn.com>

Wed, 31 Mar 1999 12:02:48 +0100

The UK changed to Summer Time (GMT+1 = BST) at 02:00 hours on Sunday 28 March 1999.

A national newspaper printed a warning in the TV listings, that VCR owners should not adjust the clock on their VCR until 06:00 as alteration (to BST) would invalidate the settings of the Video Plus+ system. This is a system whereby a code number is assigned to each programme (identifying channel, start day and time, and duration). This number can be entered into the VCR (via the remote control) and it automatically records the programme(s) as programmed.

My VCR takes its clock from the broadcast Teletext system and adjusts the time automatically. As warned, any programming of the Video Plus + system would thereby be invalidated. The impact of this RISK is minor, but extend the application ...

✶ Brain-dead PacBell automated payment promise system

"Michael D. Crawford" <crawford@goingware.com>

23 Mar 1999 23:19:31 GMT

I just got a recorded message telling me to call Pacific Bell at an 800 number about my overdue bill.

I've had rather amazing phone bills for the last year because my girlfriend lives in another country.

I sent them \$1100 on March 20, so I figured I could call and just say the check was in the mail. Today's the 23rd.

After navigating through the maze, entering my phone number and the last four digits of my social security number, I was told that I could send the bill in two parts. I selected the option to mail it. Then when asked to enter the date I would be mailing it as 4 digits, I entered 0320. The machine asked if I meant meant March 3, 2000? No, I meant three days ago. Entering 0324 was acceptable to the machine, which is apparently unable to conceive of the concept "the check is in the mail".

Then it said I needed to mail in \$164.88. I entered that I

would send in
\$200, just because I couldn't remember how much I needed to send
in. It said
that was unacceptable, the minimum due was \$164.88. That time I
remembered
it and entered in \$164.88. It said that was unacceptable, the
minimum due
was \$164.88, so I hung up.

The amount that's actually past due is \$900, so that will be
covered when the
check is received. I figure if the money's important enough for
them,
they'll call me with a real human about the arrangements.

--

Michael D. Crawford
GoingWare - Expert Software Development and Consulting
crawford@goingware.com
<http://www.goingware.com>

✂ Re: Unusable backup power (Weingart, [RISKS-20.24](#))

"Terry Harris" <tharri11@bellsouth.net>
Fri, 2 Apr 1999 11:30:59 -0600

This is a multi-part message in MIME format.

Some years ago a friend worked at a site with an IBM 370/145.
The site
handled DP for several hospitals. They decided they wanted a
backup power
source to prevent interruptions in service. They had a battery
based system
installed that would give them several hours of operation. The
backup
system produced 208V 3 phase current at 60Hz.

It turned out that they and the backup system supplier had
forgotten one

thing. The 370/145 actually ran on 208V 3 phase 400Hz. The 370 included a motor-generator set to convert the current (a 60Hz motor connected to a 400Hz generator). These motor generator sets had a considerable startup current (initially about 375 Amps decreasing to about 20 over a few seconds) and the backup system could not supply that much.

If the backup system switched in fast enough that the generator did not spin down the computer was still useful. If the backup power switch wasn't fast enough it did no good as the computer could not be restarted.

The moral: understand all the requirements that the backup system will have to meet.

⚡ Origins of PC / Mac Virus Vulnerability

Mich Kabay <mkabay@compuserve.com>

Wed, 31 Mar 1999 16:58:47 -0500

Letter to the Editors, ATLANTIC MONTHLY.

Dear Editors:

I enjoyed Robert Buder's historical overview of the rise of computer viruses (April *Atlantic*) -- a particularly timely contribution to public knowledge given the explosive spread of the Melissa virus and similar e-mail-enabled nuisances in late March 1999.

Unfortunately, technologically unsophisticated readers may have concluded that computer viruses are inevitable outgrowths of the nature of

computers.

Now, any author must select what to include or not, especially when writing within a word-count limitation. As a contribution to the discussion, not as a criticism, I did want to add a couple of fundamental points that were not mentioned in the article but that may help readers understand why we are suffering this cyberplague.

1) Computer viruses in the wild exist almost exclusively on Microsoft DOS, Microsoft Windows 3.x, 95, & 98 and Apple MacOS operating systems. For all practical purposes, there are no viruses in UNIX, MVS, VMS, MPE and other operating systems that run on workstations, minicomputers and mainframe computers. The root (no pun intended) of our PC virus woes is design decisions made long ago. Microsoft engineers decided to dispense with a security kernel -- the part of the operating system that determines exactly what kinds of operations an ordinary user is permitted to perform. The security kernel limits certain other operations to supervisory users (often known as "root") and yet others to the operating system itself. In well-behaved operating systems, changing a memory location (for example) is usually a restricted operation. Under Windows95, in contrast, every user is in effect root and programs the user runs can do anything at all. Without this vulnerability, viruses in the PC and Mac worlds would be severely limited in their effects (the "payload").

When PC and Mac operating systems introduce a security kernel into their

operating systems, much of the viral payload would be defused.

2) Microsoft engineers decided to turn office software into a general programming tool. MS-Office programs include macros -- not an unusual feature for word processors and spreadsheets in the last 20 years.

Unfortunately, they also decided to allow two functions that made their software vulnerable to macro viruses: (a) automatic execution at startup; and (b) access to system routines. Without these features, Word and Excel macro viruses would not be as powerful nor as virulent in their replication as they are today.

When Microsoft changes the defaults on Word and Excel to prevent automatic execution of macros, PC and Mac viruses will have greater difficulty in replicating.

Public awareness of the design decisions underlying our vulnerability may help sway software engineers towards improvements in our working environment.

M. E. Kabay, PhD, CISSP, Director of Education, ICSA Inc. --
Vermont
255 Flood Road Barre, VT 05641-4060 <<http://www.icsa.net>> 802-479-7937

✉ Re: More e-mail risks (Brown, [RISKS-20.28](#))

Michael H Buselli <cosine@computer.org>
Fri, 02 Apr 1999 11:21:31 -0600

> 1. If too many people use this thing, we may get spamming
incidents in
> which the spammer adds a PostPet attachment to the spam, ...

I think risk readers should know that Microsoft Outlook does
this kind of
thing now. If you want to get a guaranteed reply when someone
using Outlook
as their mail client looks at your e-mail, add the following
header:

```
Return-Receipt-To: Michael H Buselli <cosine@computer.org>
```

Now, I've noticed that Outlook ignores the address given by this
header
and uses the address specified by the "Sender:" header instead,
but
that's not difficult to set to be whatever you want.

I used Outlook 98 to perform my tests playing with this header.
I suspect
that all other versions do the same. I am not familiar enough
with Outlook
Express to know if the risk applies to that mail client as well.

Perhaps there should be an option in Outlook to confirm or turn
off these
auto-responses?

Michael H Buselli cosine@computer.org || <http://www.enteract.com/~cosine/>

🔥 Re: Apple Y2K (Stringer-Calvert, [RISKS-20.28](#))

Art Delano <ajd@home.msen.com>
Fri, 2 Apr 1999 09:33:33 -0500

> "We may not get everything right,
> but at least we knew the century was going to end."

> -- Apple Computer, HAL 9000 ad for Macintosh Y2K compliance

To the best of my knowledge, that wasn't used in the Apple's Superbowl commercial (the commercial is available online for download, but i feel lazy). On the other hand, the same quote had been circulating, attributed to Douglas Adams, for at least half a year.

A quick check with a search engine didn't turn up the original context of the quote, but did find Apple's citing Adams on their own website:
<http://www.apple.com/about/year2000/> -- as an introduction to their own Y2K compliance statement.

Incidentally, Apple's statement that currently-supported hardware and software are Y2K compatible allows them to make preemptive decisions to discontinue support for any products they may decide are better dropped than revised. While they're hardly the only company to do this, they might at least provide documentation of what has been discontinued and recommend upgrade paths, to keep their customers from guessing at what they need.

As has already been observed, even if a supported system, as shipped, will be Y2K-compatible, third-party software may not be. Users may not be willing to spend money and time and effort replacing working software with other working software that provides no apparent outward improvements. I have doubts that the average computer-using consumer has a clear understanding of the distinctions between disparate applications, utilities, and system

functions, particularly in our current era of 'seamlessly' integrated software, and will blame all problems at whichever company seems to have their name most prominently displayed on the package. The confusion is probably better left as a subject for another thread.

ajd@boutell.com

[Also noted by DeRobertis <derobert@erols.com>. PGN]

✶ REVIEW: "Information Warfare and Security", Dorothy Denning

Rob Slade <rslade@sprint.ca>

Tue, 23 Mar 1999 08:44:02 -0800

BKINWRSC.RVW 990212

"Information Warfare and Security", Dorothy Denning, 1999,
0-201-43303-6, U\$34.95/C\$52.50

%A Dorothy Denning denning@cs.georgetown.edu

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8

%D 1999

%G 0-201-43303-6

%I Addison-Wesley Publishing Co.

%O U\$34.95/C\$52.50 800-822-6339 Fax 617-944-7273 bkexpress@aw.
com

%P 522 p.

%T "Information Warfare and Security"

Denning has chosen to take an inclusive approach to the topic of information warfare, not limiting the material to attacks on "military" targets. Given the state of physical warfare, this seems to be quite realistic. It does mean that the book tends to read like a high level computer security text (small wonder) with an emphasis on

intrusions and the more overt aspects of computer crime.

Part one is a foundation and background for the material to come. Chapter one looks at the great many information aspects to the Gulf

War and Operation Desert Storm. One of the unusual factors reviewed

is that of propaganda, or "perception management." A theory of infowar is the intent of chapter two, which outlines players and positions in a variety of ways. The theory is somewhat weakened for

being strongly dependent upon the idea of the value of the information

being attacked or defended, and this is an area that still requires

work. Another possibly problematic area is the reliance on a "win-

lose" model for data warfare, when there have been numerous instances

of intruders, upon sufficient provocation, being willing to deny themselves a resource by damaging it, on the basis that the defenders

stand to lose far more. (On the other hand, "bragging rights" seem to

have a lot of value in the computer underground.) More detail on the

players involved, and the possible types of attacks that have occurred, and might occur, are presented in chapter three.

Part two looks at the specifics of offensive information warfare.

Chapter four is extremely interesting, showing that "open source," or

publicly available information, can and has been used for offensive

and criminal undertakings in a variety of ways. Disinformation is

reviewed in chapter five, including the odd phenomenon of urban legends and Internet hoaxes. The problem of damage from insiders,

including, finally, a documented case of a salami attack (albeit a

rather clumsy one), is covered in chapter six. Chapter seven

discusses the interception of information and communications in a

variety of ways, and, as a sideline, jamming and alteration. A variety of methods of computer intrusion are presented in chapter eight. False identity, both identity theft and outright false, are examined in chapter nine. The material on viruses and worms, in chapter ten, is solid, although I was sorry to see that a great many possibilities for reproductive mayhem that have been discussed over the years went unmentioned. ("Harlie," Dr. Denning. "When *HARLIE* Was One.") (Of course, when I sent the first draft, I had, myself, spelled "Harlie" incorrectly.)

Part three looks at the opposite side, that of defence. Chapter eleven gives a good background to encryption, but, seemingly, primarily as a general concept, rather than going into detail on specific uses for protection. Authentication is dealt with in chapter twelve, and uses some of the cryptologic background. With monitoring and detection bracketing chapter thirteen, the section on firewalls seems just slightly misplaced. Chapter fourteen looks at risk analysis, planning, and some resources. The final chapter discusses defence of the nation, and national policy in this regard, with particular emphasis on the current situation in the US.

The content of this book not only presents a clear picture of a number of aspects of information warfare, but does so in a very practical manner, informed by the need to use "real world" examples. In addition, the anecdotal evidence backing the material makes the book quite readable and interesting. As a text for a course in information warfare, it is complete and solidly based. As a reference for security analysts and practitioners, it is clear and thought-provoking. For those who may merely have some interest in the topic,

it is engaging and informative.

copyright Robert M. Slade, 1999 BKINWRSC.RVW 990212
rslade@vcn.bc.ca rslade@sprint.ca robertslade@usa.net
pl@canada.com

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



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 30

Friday 16 April 1999

Contents

- [Fake web page cause 20% stock surge and then retreat](#)
[Avi Rubin](#)
- [Glitch causes 4 billion euro overdraft](#)
[Monty Solomon](#)
- [Raytheon probes e-mail moles](#)
[Keith A Rhodes](#)
- [Security is still a human problem](#)
[Jeremy Epstein](#)
- [Y10K: not just for April Fools](#)
[Tom Swiss](#)
- [The Risk of 1 Apr](#)
[David Frank](#)
- [RISKS April Foolery, Melissa, security, and frequencies of RISKS](#)
[PGN](#)
- [GPS setup error affects dredging in California](#)
[W.T. Shymanski](#)
- [Potential RADHAZ](#)
[Paul Walczak](#)
- [Space character in number causes silent Excel miscalculation](#)
[Ben Bederson](#)

- [Security Hole in Java 2](#)
[Gary McGraw](#)
 - [Re: Vancouver Hospital](#)
[Doneel Edelson](#)
 - [Microsoft reschedules Memorial Day](#)
[Benjamin B. Bederson](#)
 - [Risk of not backing up PGP Key Ring files](#)
[Herman D. Knoble](#)
 - [Responses to Melissa](#)
[Chuck Karish](#)
 - [Risks of "Melissa passed this way"](#)
[Charles Arthur](#)
 - [Melissa and poor security model of Word Macros](#)
[Scott M Keir](#)
 - [Mainframe virus](#)
[Henry Schaffer](#)
 - [Millennialism in the Western Hemisphere](#)
[Richard Landes](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Fake web page cause 20% stock surge and then retreat

Avi Rubin <rubin@research.att.com>

Thu, 8 Apr 1999 19:38:42 GMT

There is a story in **The New York Times** 8 Apr 1999 about a web spoof that cost people serious money. Apparently, somebody set up a Web page that looked exactly like a commercial financial Web site. The claim was made that PairGain Technologies (PAIR) was set for a takeover. On this speculation, the price shot up 20% the same day. Once the hoax was proven, the stock came back down, but presumably not all the people who bought high

got out on time.

While such an event is unfortunate, there is a taste of "I told you so" to see that one of the dangers we've been preaching about for so long actually caused loss of revenue. I believe this is the first of many such swindles to come.

Avi Rubin

[Also noted by Jim Reisert. A PairGain employee, Gary Dale Hoke was subsequently arrested at home in Raleigh NC, despite an effort to access the Internet anonymously'', according to the *San Francisco Chronicle, B1, 16 Apr 1999. PGN]

⚡ Glitch causes 4 billion euro overdraft

Monty Solomon <monty@roscom.com>
Tue, 13 Apr 1999 01:16:57 -0400

Glitch causes 4 billion euro overdraft (IDG, 12 Apr 1999)
by Mary Lisbeth D'Amico

Although the January switch to the single European currency was smooth at most European banks, a prominent German discount bank and its customers this week were acutely aware that not all possible euro-caused glitches have been found. Customers of Bank 24, a discount bank owned by Deutsche Bank AG, were astonished [on 6 Apr 1999?] to find that their securities accounts appeared to be overdrawn to the tune of 4 billion euro (\$4.32 billion). An

oversight connected to the change to the euro was responsible for the error, affecting 55,000 customers.

<http://www.cnn.com/TECH/computing/9904/12/overdraft.idg/>

✶ Raytheon probes e-mail moles

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

Mon, 05 Apr 1999 15:35:31 -0500

Yahoo! subpoenaed to identify messagers; Raytheon execs resign

At least two Raytheon employees have resigned in the wake of proprietary messages appearing on Yahoo message boards. Raytheon is accusing 21 employees, and has subpoenaed Yahoo! to the identify the senders of anonymous e-mail. [Source: CNNfn, 5 Apr 1999, PGN-ed]

✶ Security is still a human problem

"Epstein, Jeremy" <Jeremy_Epstein@NAI.com>

Mon, 12 Apr 1999 14:32:47 -0700

Just in case you thought that security problems were solved by computers, we're reminded yet again that it all comes down to trusted people doing the right thing. I wonder if John Deutch got a copy of the Melissa virus, potentially sending classified files to his closest friends?

A routine check of former CIA Director John Deutch's home turned up

31 files classified secret on his personal computer after he had stepped down and was retained as a consultant. No prosecution is planned, because the violations were not deemed criminal. [PGN-ed from various sources, mostly Associated Press, 11 Apr 1999]

✶ Y10K: not just for April Fools

Tom Swiss <tms@infamous.net>
Sat, 3 Apr 1999 21:09:06 -0500

So maybe I'm an April Fool, but it seems to me that the Y10K issue is worth a little serious thought.

There are areas of human endeavor in which 8000 years is not an extreme time span. At present, we deal with these long time spans only in modeling things like geological and cosmological events. But it is not unreasonable that within the next century, we may begin to build very high technology systems with mission durations of thousands of years - for example, a system to contain radioactive wastes, or a probe to another star system.

Y2K issues have raised our consciousness about timer overflows, but it's quite possible that this may fade in succeeding generations. There's no reason not to start setting standards now.

Perhaps all time counters should be bignums?

== Tom Swiss/tms@infamous.net == <http://www.infamous.net>

⚡ The Risk of 1 Apr (Re: Computer crash creates nonpersons in Zurich)

"David Frank" <David.Frank@access.unizh.ch>

Wed, 07 Apr 1999 23:12:00 +0200

I'm hardly the first to point this out, but there is a certain risk in

- a) abstracting too much and
- b) doing this on 2. April and
- c) doing it with articles on such risk-worthy topics ;-)

Why? This story makes perfect sense to any Risk-Reader but it's an April

Fool's joke. (I myself expected them, but this one is hardly detectable.)

The **Tages-Anzeiger** story goes on telling people to go to the townhall and

register themselves to avoid losing their citizenship.

Anyway: you should have backup tapes!

David Frank, Dietlikonerstr. 14, CH-8304 Wallisellen, Switzerland
+41 (0)1 830 6506, David.Frank@access.unizh.ch

[Unfortunately, not all of the 1 Apr material is on hand in time.]

⚡ RISKS April Foolery, Melissa, security, and frequencies of RISKS

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

Fri, 16 Apr 1999 10:16:08 PST

Regarding the plethora of foolacious items in [RISKS-20.26-29](#), RISKS has a

general policy of NOT explicitly identifying foolish material
around 1 Apr

each year. You are all on your own, and expected to read
discriminatingly.

Besides, sometimes the most ridiculous sounding risks are quite
real.

I received a few pieces of e-mail questioning the validity of
one particular
item or another, which suggests to me that some of you must have
taken many
of the other items as genuine! This is somewhat surprising, but
will not

alter our policy in future years. An unexpected exception to
this policy

was Lauren Weinstein's Inside Risks column on the risks of
teleportation in

the April 1999 issue of the Communications of the ACM. Although
neither he

nor I wanted any explicit April Foolish disclaimers on the
column, our CACM

editor decided to add an explicit warning -- perhaps fearing
that some of

you were ready to try this technology anyway. For those of you
who are not

CACM subscribers, Lauren's column is on my Web site, Start with
<http://www.csl.sri.com/neumann> and click on "Inside Risks".

Also on my Web site (<http://www.csl.sri.com/neumann/house99.html>) is my

testimony for yesterday's hearing of the House Science Committee
subcommittee on technology, in which I consider Melissa as the
tip of a very
large iceberg -- the abysmal state of computer and communication
security.

My testimony, plus that of Keith Rhodes and others, will also be
at

<http://www.house.gov/science/welcome.htm> -- click on committee
hearings,

then subcommittees, and find the 15 Apr hearing, supposedly by
the end of

the House working day EDT.

Incidentally, newer readers sometimes ask why RISKS comes out so irregularly. The answer of course is that I run it in odd moments, whenever I can. If you ever think you missed an issue or think that your subscription might have been dropped, please check the various RISKS Web sites and mirrors for the latest issue. (Even when I prune the list militantly from previous invalid addresses, I sometimes receive as many as 300 bounces on the next issue. I gather that USENET loses an issue now and then as well.)

✶ GPS setup error affects dredging in California

"W.T. Shymanski" <wtshyman@mb.sympatico.ca>

Sat, 03 Apr 1999 17:04:39 -0500

The 22 Feb 1999 "Engineering News Record" in an item titled "Dredge spoil misplaced due to alleged GPS programming error" reports that 600,000 cubic yards of dredged spoil were dumped almost half a mile from an approved site, off the coast of Orange County, California, due to an error in keying in co-ordinates into a GPS receiver.

A new GPS unit had been installed on a tug, and apparently the operator keyed in the co-ordinates in base 60 (degrees, minutes, seconds) instead of in base 100 (degrees, minutes, decimal fraction of a minute) that the new GPS used. The error was detected when the crew of the tug noticed another tug and barge dumping spoil in the approved site.

Misinterpretation of the display units of measurement is a

fairly common
problem in user interface design and is probably responsible for
no end of
wasted paper, misprogrammed VCRs, and in at least one case (the
767 "Gimli
Glider" incident) a serious threat to air safety.

W. T. Shymanski <wts@ieee.org>

✈ Potential RADHAZ

<Paul_Walczak@mail.arl.mil>

Thu, 8 Apr 1999 13:42:06 -0400

[From an anonymous source]

I worked with the PRC-138 for over 5 years now. I was teaching
some Korean
soldiers how to operate it with a wire antenna hanging out the
window. Well
this is not the most optimum antenna and it provide not to be by
being able
to watch smoke start curling off my finger tips while operating
the radio.
The manual on this radio states that the radio must be grounded
and the 20
watt manpack set comes with a strap and small ground rod. The
PRC-104 has
this same problem if you build a poor antenna that the radio
cannot match
to. It probably stand the same that 125 watt systems in
vehicles need to be
grounded also.

Subject: [SIGNET] AN/PRC-138 Potential RADHAZ

1. Testing of the AN/PRC-138 HF radio by the Canadian Military
has revealed
a non-ionizing radiation hazard.

2. This message is posted to inform you and to find out if any similar incidents have occurred with radios with US forces. Also, if this condition is known, what are we doing about it to prevent this hazard?

3. The Canadian PM for the 138's received reports from users in Bosnia that electrical shocks were received from the AN/PRC-138 in a man-pack configuration and when used as a temporary communications system in a vehicle. It had also been reported that electrical shocks were being experienced by users of the 138 when installed in a vehicle mounted 125 Watt Power amplifier system in the Canadian ILTIS (jeep-type) vehicle.

4. The investigation revealed the AN/PRC-138 radio produced electrical shock/RF burn hazards when configured as a man-pack or installed as in the ILTIS in the 125 Watt configuration. A man-pack operator would feel electrical sensations from any conductive part on the radio front-panel and uninsulated screw on the handset during transmission. The investigation also revealed that the sensations were worst when humidity conditions were dry. In the ILTIS, the RF burn sensation was not limited to the radio equipment but also any other uninsulated and ungrounded conductors such as a watch bracelet. The electrical sensations created by the contact current could also cause a knee-jerk reaction which in itself could cause an accident.

5. The man-pack tests utilized the radio at 20 Watts over several frequencies with both the whip antenna, model number AT271A/PRC (NSN

5985014248333) and the dipole antenna, model 1903AD (NSN 5985013567620). A safe distance of 0.75 metres from the whip and 1.5 metres from the dipole transmitting antennae was measured. In order to eliminate any potential confusion when antennae are exchanged, a safe distance of 1.5 metres should be observed for both antennae.

6. Personnel requiring more information or a copy of the complete test results should send their requests to the undersigned.

Major RK (Kevin) Ferguson
Canadian Forces Liaison Officer - Signals
714 Signal Towers
Fort Gordon, GA 30905-5680

Phone: Comm (706) 791-4163
 DSN 780-4163
Fax: Comm (706) 791-7829
 DSN 780-7829
E-Mail: fergie@emh.gordon.army.mil

⚡ Space character in number causes silent Excel miscalculation

"Ben Bederson" <bederson@cs.umd.edu>
Thu, 15 Apr 1999 17:50:14 -0400

Error of US\$19,130 !

I have found Microsoft Excel to be very good at mixing different data types without having the user to specify those types. However, the fact that the types are not specified explicitly pose a risk. I recently had a budget submitted and approved that turned out to add up to US\$19,130 over what the

grand total said it did. The problem was that the \$19,130 item was actually listed as "19, 130" The space character was barely distinguishable on the screen (partially because of the use of a proportionally-spaced font and the fact that the space was directly after a comma). It was only when I printed the spreadsheet later on that I noticed it (after the budget was approved).

Normally, this error stands out because Excel by default left-justifies text and right-justifies numbers. However, I had specifically right-justified the column in question earlier. The issue here is that the "19, 130" was interpreted by Excel as text rather than as a number. Since Excel doesn't generate warnings when adding text, but rather interprets it as 0, I had no notification of the problem.

This is an instance of a general risk in the trade-off that often comes with making interactive systems usable in that many mundane tasks are automated (such as type specification), and warnings are eliminated resulting in the user not knowing how things are interpreted.

Prof. Ben Bederson, Computer Science Department, HCIL,
University of Maryland
College Park, MD 20742 1-301-405-2764 www.cs.umd.edu/~bederson

Security Hole in Java 2

Gary McGraw <gem@rstcorp.com>
Mon, 5 Apr 1999 08:57:43 -0400 (EDT)

Karsten Sohr <sohr@mathematik.uni-marburg.de> at the University of Marburg in Germany has discovered a very serious security flaw in several current versions of the Java Virtual Machine, including Sun's JDK 1.1 and Java 2 (a.k.a. JDK 1.2), and Netscape's Navigator 4.x. (Microsoft's latest JVM is not vulnerable to this attack.) The flaw allows an attacker to create a booby-trapped Web page, so that when a victim views the page, the attacker seizes control of the victim's machine and can do whatever he wants, including reading and deleting files, and snooping on any data and activities on the victim's machine.

The flaw is in the "byte code verifier" component of the JVM. Under some circumstances the verifier fails to check all of the code that is loaded into the JVM. Exploiting the flaw allows the attacker to run code that has not been verified. This code can set up a type confusion attack (see our book "Securing Java" for details <http://www.securingjava.com>) which leads to a full-blown security breach.

We have verified that the flaw exists and is serious. Attack code (in both applet and application form) has been developed in the lab to exploit the flaw. Sun and Netscape have been notified about the flaw and they are working on a fix.

What?! RISKS in mobile code? We're happy to alert you to yet another lesson regarding the classic tradeoff between security and functionality.

Dr. Gary McGraw
Reliable Software Technologies
Lab
gem@rstcorp.com

<http://www.securingjava.com>

Prof. Edward W. Felten
Secure Internet Programming

Dept. of Computer Science
Princeton University
felten@cs.princeton.edu

[Reportedly fixed in 1.2.1. PGN]

✦ Vancouver Hospital (Re: [RISKS-20.23](#))

"Edelson, Doneel" <doneeledelson@aciins.com>

Thu, 18 Mar 1999 12:07:39 -0500

I spoke with Mr. Lee on the phone and he said that he stands by his story.

He also said that some of the specific wording in the Risks Digest summary

of the story was significantly different from his actual story.

He also requested that the Risks Digest not carry any more material from his

column. To that end I plan to no longer forward his column to you.

Here is my statement on the matter. I am CC:ing the hospital, and plan to

send them a copy of the actual posting from Risks when it is published.

[Sorry for the delay. I've been away too much. PGN]

In [RISKS-20.23](#), I noted a report from Leonard Lee's Glitches of the week,

Newsbytes News Network<<<http://www.newsbytes.com/>>>, 24 Feb 1999, concerning

problems in the Vancouver Hospital computer system that resulted in errors

in patient medical records. In response, I received the following communication from Murray T. Martin, President & CEO of Vancouver Hospital:

"As you are in error, we write to ask you to remove the postings, to apologize to VHHSC, and to initiate steps to advise those who may have accessed the information. Vancouver Hospital and Health Sciences Centre takes very seriously these defamatory statements, and has advised the software vendor of our concerns. We reserve the right to take legal action on the alarming and libelous statements.

In particular, your statement as fact that the software and process errors had the effect of "significantly delaying treatments and discharges, and increasing costs" is incorrect and defamatory. There is no evidence to our knowledge of any of these effects, and ask that if you have such evidence, you provide it to us."

I apologize to Vancouver hospital for any harm that this has caused.

Microsoft reschedules Memorial Day

"Benjamin B. Bederson" <bederson@cs.umd.edu>

Thu, 8 Apr 1999 09:59:10 -0400

Microsoft Outlook 98 has scheduled Memorial Day for May 24, 1999 instead of May 31, 1999. I thought this kind of power was reserved for the Federal Government! According to my Microsoft contact, this feature is included in Office 2000 as well - and so apparently there is not much quality assurance in the data that Outlook comes with.

This is actually a fairly serious problem for those of us that rely on Outlook. I managed to schedule a visitor coming from another Country to give a talk on what turns out to be Memorial Day. If the plane tickets the visitor bought are non-refundable, we could have some trouble. I'm sure that the Microsoft licensing agreement absolves them from responsibility for this kind of error. So, the risk is, make sure you trust your data sources...

Prof. Ben Bederson, Computer Science Department, University of Maryland,
College Park, MD 20742 www.cs.umd.edu/~bederson 1-301-405-2764

⚡ Risk of not backing up PGP Key Ring files

Herman D. Knoble <hdk@psu.edu>
Wed, 07 Apr 1999 14:04:35 -0400

A professor and psychologist at Penn State kept state mandated records for each client in a separate Word file. He obtained PGP 5.0 for Windows 95 and set up a Username and Passphrase. He then used PGP to encrypt each client file. He backed up the encrypted client files and after reassuring himself that he could recover any encrypted file, he erased the plain text files.

Then his fixed disk crashed. He installed a new fixed disk and installed PGP 5.0 again, and attempted to re-establish what he called "the key" by using the same Username and Passphrase. He had never backed up the

key ring file
(secring.skr) thinking that he could re-create what he thought was "the PGP key". Needless to say his 150 or so encrypted client records are not decipherable. Thus, for all practical purposes, that data is lost and the encrypted files may as well be erased.

Moral: When encrypting any data, find out how to and what to back up for BOTH the data and key(s) . Then secure each of these backed up media, probably under lock and key, with a copy not in the same building as the computer. At least periodically verify that backed up data can be decrypted successfully on an independent computer.

Herman D. Knoble, Penn State Center for Academic Computing,
University Park,
PA 16802-2101 +1 (814) 865-0818 hdk@psu.edu <http://www.personal.psu.edu/hdk>

⚡ Responses to Melissa

Chuck Karish <karish@well.com>
Mon, 05 Apr 1999 01:24:07 -0700

This evening I watched an item on the Melissa virus on a cable TV technology newsmagazine show. The reporters talked to someone at a company that monitors Internet performance, who attributed two days during which performance was degraded by 20% to 23% to many downloads of virus checking tools and information about the virus.

Then they asked people from a virus-checking software company how to defend against such viruses. They said "Always run a virus checker, and update your database frequently".

This struck me as being incomplete. Why does virus defense have to be reactive? I'd heard that Microsoft has a free downloadable Word viewer that wouldn't have the macro security hole. So, off to the Microsoft Web site.

The prominently-displayed short note there on Melissa wasn't much different from what the virus-checker guys said on TV. "Turn off macros, use a virus checker, update it frequently." No mention of what to do if your machine has already been infected (so that turning off macros might not be possible), no mention of a macro-ignorant doc viewer.

I found the download index that showed the Word document viewer. Unfortunately I couldn't download it, because my browser (IE4.0) reported a programming error in the download page.

So, I settled for downloading a white paper on security features in Office 2000. This was a Word document packaged in a self-extracting executable program. Not the ideal format to inspire confidence in this reader! The paper (o2ksec.exe) does contain useful information, including the registry settings to disable VBA macros or add-ins, and suggestions for locking critical sections of the registry without interfering unduly with user activities. Any guesses as to how many sysadmins and self-admins will follow those instructions?

Doesn't anybody get it?

Chuck Karish

karish@well.com

(650) 329-8655

⚡ Risks of "Melissa passed this way"

"Charles Arthur, The Independent" <carthur@independent.co.uk>

Thu, 8 Apr 1999 15:36:57 +0100

Big financial institutions were quick to put in place automated safeguards against the Melissa virus. Which didn't explain why one coworker received an e-mail on Tuesday, eight days after the affair hit most UK sites, headed "Important message from GWUser". It came from GWUser, who (the address showed) was based at a UK "Big Four" high street bank. In fact, it was Melissa-generated.

The mail itself though did not contain the dreaded document, nor any document; instead there was a message from the Bank's virus-checking software saying it had removed the document. The address list, meanwhile, showed 25 addresses - some inside, some outside the Bank (such as ourselves).

However, almost simultaneous with this message came another one, by automaton, from the Bank's security systems. "You have been infected by the Melissa virus", it said (I'm busking a little - the colleague has since deleted them). This message had been sent out to all the recipients on the same list. The implication of the message was that it couldn't

identify the source of the message it was complaining about as being inside its walls, and was blaming us for sending it, rather than warning us.

Even so, two clear risks:

- 1) doubling the load on mail systems by having two messages, even though the virus-checker did do its work and killed it (thus saving further propagation);
- 2) confusing the hell out of recipients who aren't savvy enough to follow what had happened - which included the original colleague here.

We however have reason not to worry about this. We run Macs, use an old version of Word without macros but with forward compatibility, and use Lotus Notes rather than Exchange or OExpress. Virus writers have not expanded to fill that particular niche, if they ever can/will.

Charles

[Melissa and poor security model of Word Macros \(Waide, RISKS-20.26\)](#)

Scott M Keir <scott@tardis.ed.ac.uk>
Tue, 6 Apr 1999 18:46:50 +0100 (BST)

> 4 Microsoft praised for having GUIDs in documents.

I certainly hope that 4) is followed by:

5 Microsoft is condemned for developing a language with a poor security model.

That Melissa can disable security-related menu commands and alter the 'security' features of the macro language interpreter shows what a poor security model the language has. Perhaps this was acceptable when the macro language was used for simple templates in documents, but with the emergence of macro virii and the expansion of the language to fairly effectively control the machine, this is not acceptable any more.

Cross-platform languages such as Tcl and JavaScript have some security model which attempts to reduce the ability of code to damage your system in some way (e.g. Tcls Safe-Tcl security model is now fairly advanced, and allows users to run scripts in 'Safe Mode' preventing scripts from accessing sensitive parts of the machine).

That any 'security' in Word macros can appear to be overridden by macros is poor show on Microsoft part. They need to fix this, and soon.

Scott Keir scott@tardis.ed.ac.uk www.tardis.ed.ac.uk/home/scott/ |

[Incidentally, there is confusion among the various news reports of

Melissa as to exactly when and how the GUID entered into the identification of the perpetrator. Can anyone who really knows enlighten us? PGN]

✶ Mainframe virus (Kabay, re: [RISKS-20.29](#))

<hes@unity.ncsu.edu>

Fri, 9 Apr 1999 21:27:19 -0400 (EDT)

The Christmas Tree "virus" affected VM systems some 10+ years ago. (IIRC it really affected PROFS.) I think it is reasonably comparable to Melissa.

> Microsoft engineers decided to dispense with a security kernel ...

If a computer has an integrated word processor in its mail software, then it very well might not take supervisor privileges for a word processor macro to send mail. I think this was the source of the PROFS vulnerability.

--henry schaffer

⚡ Millennialism in the Western Hemisphere

Richard Landes <cms@mille.org>

Wed, 7 Apr 1999 13:09:48 -0400

CALL FOR PAPERS

The Center for Millennial Studies at Boston University in conjunction with the American Studies Department at Brandeis University announce the upcoming conference sponsored by the Lilly Endowment Foundation, Boston University, and Brandeis University.

NEW WORLD ORDERS: MILLENNIALISM IN THE WESTERN HEMISPHERE
November 7-9. 1999

An interdisciplinary inquiry examining the wide range of millennial movements in the Americas: their origins, traditions,

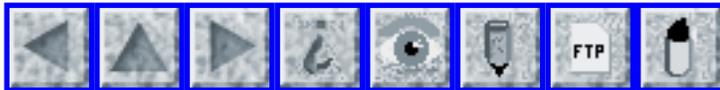
interpretations and consequences, both religious and secular from the perspective of elite, popular, or counter-culture. Papers on the historiography of millennialism in the Americas will also be considered for presentation.

DEADLINE For Abstracts Is JULY 1, 1999 [presentations 20 minutes in length]

Contact:

Beth Forrest, Center for Millennial Studies at Boston University
704 Commonwealth Ave., Suite 205, Boston, MA 02215
1-617.358.0226 cms@mille.org <http://www.mille.org>

[Richard and his CMS colleagues at Boston University are looking at the BIGGER PICTURE of Millennialism! 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 20: Issue 31

Sunday 18 April 1999

Contents

- [BART ghost train snarls morning commute](#)
[PGN](#)
- [EMI from USS Carl Vinson opens garage doors in Hobart](#)
[Norbert Thumb](#)
- [ASerbic cyberattacks and counterattacks](#)
[PGN](#)
- [Fake ATM front panel copies cards and PINs](#)
[Ulf Lindqvist](#)
- [Overzealous applications](#)
[Ian Cargill](#)
- [Outlook '98 not Y4.501K Compatible](#)
[Eric Zago](#)
- [favicon.ico](#)
[Robert David Graham](#)
- [Leap year 2000 and C](#)
[Mark Brader](#)
- [Risks of April foolery](#)
[Pete Mellor](#)
- [GUIDs and Melissa](#)
[Robert David Graham](#)

- [Phone company says keep your PIN on your calling card](#)
[David Graf](#)
 - [Re: Mainframe viruses](#)
[Julian Thomas](#)
 - [E-mail and communications history](#)
[Dennis Ritchie](#)
 - [REVIEW: "Hacker Proof", Lars Klander](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **BART ghost train snarls morning commute**

"Peter G. Neumann" <neumann@csl.sri.com>
Sat, 17 Apr 99 13:16:33 PDT

On 16 Apr 1999, a ghost train appeared in the BART computers on a section of track between the Montgomery and Embarcadero stations in San Francisco. BART continued to operate manually on that stretch of track for about 4 and one-half hours through the morning rush-hour. Although this is not news to commuters, what seems startling was a recent consultant's report, which documents 567 such incidents in a two-year period. (We also reported repeated appearances of ghost trains in the Muni Metro system about 15 years ago.)

⚡ **EMI from USS Carl Vinson opens garage doors in Hobart**

Norbert Thumb <thumb@ict.tuwien.ac.at>
Sat, 17 Apr 1999 23:37:50 +0200

As the aircraft carrier USS Carl Vinson approached port in Hobart, Australia, last week, its communications at 310-320 MHz jammed most garage-door openers within 6 miles. (The same thing happened on the Vinson's previous visit. Most garage doors have manual overrides.) The EMI also immobilized the "shielded" car security system of a resident near the docks, whose car could not be started -- no manual backup there. [Source: US Navy Closes Doors Down Under, by Stewart Taggart, 16 Apr 1999, Anonymously contributed to cypherpunks; PGN-ed]

Dipl.Ing. Norbert Thumb, Institut f.Computertechnik, Vienna University of Technology; Austria +43/1/58801-3704 thumb@ict.tuwien.ac.at

✶ ASerbic cyberattacks and counterattacks

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

Fri, 16 Apr 1999 10:34:44 +0000

NATO announced that its Web server in Brussels had been under a PING-of-death (Packet INternet Groper) attack from somewhere within Serbia.

John Pike labeled it "a textbook example that will be cited from now on as a

low-cost, high-value attack." [Source: Serbia launches cyberattack on NATO,

Federal Computer Week, 31 Mar 1999, by Daniel Verton (dan_verton@fcw.com);

PGN-ed] The ease with which such attacks and other denials of service can be

perpetrated is one more reminder of the general flakiness of our information

infrastructures, but then RISKS readers are probably the last to be

surprised.

In a spy-vs-spy-style retaliation, various Internet denizens sent half a million e-mail bombs to www.gov.yu, the main Yugoslav Web site, before it shut down on 3 Apr 1999. There were also reports *The Boston Globe* of a U.S. group called Team Spl0it and European and Albanian penetrators changing Web sites. On the other hand, there are also reports of Russian hackers going after U.S. Navy Web sites. [Source: E-Strikes and Cyber-Sabotage: Civilian Hackers Go Online to Fight. 15 Apr 1999, by Patrick Riley, <http://www.foxnews.com/stage11.sml>; PGN-ed from a cypherpunks item courtesy of Dave Farber <farber@cis.upenn.edu>]

Riley cited some concerns that vigilante hacktivism might be misinterpreted as sanctioned government action. On the other hand, given the existing system and network flakiness, there might also be concern that what might seem to be vigilante hacktivism might actually be government sponsored! Perhaps future wars will be fought by our-hackers-vs-their-hackers in purely electronic warfare. It would save a lot in armaments, and would inspire greater system robustness that otherwise seems impossible to attain!

⚡ Fake ATM front panel copies cards and PINs

Ulf Lindqvist <ulfl@ce.chalmers.se>
Fri, 16 Apr 1999 16:47:20 +0200 (MET DST)

On the Swedish TV program *Efterlyst* (similar to "America's most wanted" and "Crimewatch UK") 15 Apr 1999, a police officer showed a fake ATM front panel that had been confiscated by Swedish Customs. The two Estonians that tried to bring the equipment into Sweden are in custody. From Finland and Denmark, there are reports of hundreds of cases of ATM fraud in which the police suspect that this equipment was used.

The equipment showed on TV consists of a metal panel with a built-in keyboard and hidden electronics, and a metal frame containing a magnetic card reader. The panel is placed on top of the existing keyboard panel of the ATM and the frame is placed around the card slot. The panel and the frame are connected with cables that are hidden behind a strip of metal. When a customer puts his or her card into the ATM slot, the card also passes through the added metal frame which reads the magnetic strip and stores the information in the hidden memory in the panel. Then, when the customer enters his PIN code on the fake keyboard, the code is of course also recorded, but pins underneath the panel push the real ATM keys, so the ATM operates normally.

From the description, it may appear that it would be very easy for anyone to discover the extra gadgets placed on the ATM. However, the TV program also showed the equipment mounted on an ATM, and it looked strikingly genuine - the colors of the panel were identical to those of the original panels etc. It should also be noted that cameras are not standard in ATMs in this

part of the world, making it harder for the victims to prove their cases.

The risk is one we have seen so many times before: You should not give away your secrets to something that might not be what it claims to be.

Ulf Lindqvist, Department of Computer Eng., Chalmers University of Technology
SE-412 96 Goteborg, SWEDEN +46 31 772 17 60 ulfl@ce.chalmers.se

🔥 Overzealous applications

Ian Cargill <ian@soliton.demon.co.uk>
Sat, 17 Apr 1999 14:34:34 +0100

In [RISKS-20.30](#), Ben Bederson described a problem caused by a space character in numeric fields in Excel. The problem was a particular risk because Excel makes a silent 'best guess' which may be wrong. I recently came across a similar risk with MS apps trying too hard to guess what you might have meant and silently getting it wrong.

My problem was in Access, but I suspect it is a general VB/VBA problem, not Access-specific.

When you enter a date, Access *FIRST* tries to interpret it according to the locale that you have set in control panel. Thus if you enter 2/4/99, it will be interpreted as 2 April 99 in the UK, 4 Feb 99 in the US, etc. Fine so far, but what if you enter an invalid date, such as 29/2/02?

You would expect this to be rejected in any locale, but in fact, Access quietly accepts this as a valid date - 29 Feb 2002!! The trouble seems to be that Access tries too zealously to find a 'correct' interpretation, so if dd/mm/yy (or mm/dd/yy) doesn't work, then it tries yy/mm/dd.

Of course, the problem goes away if you require users to enter four-digit years, but it is still unwarrantedly aggressive behaviour.

Ian Cargill CEng MBCS MIEE, Soliton Software Ltd.

⚡ Outlook '98 not Y4.501K Compatible

Eric Zago <zippy@WPI.EDU>

Fri, 16 Apr 1999 21:54:24 -0400 (EDT)

Not only does Outlook reschedule holidays (as mentioned in a previous risks), it also brings the old problem of how to identify data as null.

While in the past 9/9/99 might have been used to identify a 'null' date (making that date one of our famous y2k warning dates - now we have a new problem. In Outlook '98, the default date value is 1/1/4501 8:00 AM.

Obviously Microsoft has not learned the lesson. While it is not likely that anyone will be using Outlook '98 in the year 4501, that is not the point.

This is documented in a several books, but no mention is made as to any potential risks in using arbitrary dates as flags

So can I be the first to coin the Y4.501K Standard?

Eric Zago, Management Information Systems Major
Worcester Polytechnic Institute, Worcester, MA zippy@wpi.edu

favicon.ico

"Robert David Graham" <rob@netice.com>

Fri, 16 Apr 1999 22:11:22 -0700

In case you haven't heard, Microsoft has a new feature in IE 5.0 web browser. When you add a website to you "Favorites" (aka. Bookmarks for you Netscape users), the browser attempts to download a graphic called "favicon.ico", then show that icon along with the title of the webpage.

This has two risks.

First of all, the website owner is notified when you the page to your favorites, revealing information about yourself. A discussion of this can be found at <http://msdn.microsoft.com/workshop/essentials/versions/ICPIE5.asp>

This privacy risk is probably minor, but I've seen several press articles on the subject.

The second RISK is much more severe. Go to AltaVista (or any search engine) and search for "favicon.ico". You now have a list of 500 websites that expose their access logs. In the logs, you can find several websites that expose the URLs of CGI scripts, including passwords. Through manual searching, I found 2 sites that exposed logon information; I'm sure I can

write a program that would scan those logs to look for CGI programs and get even more. This also exposes even more privacy information because these logs often contain the Referer field as well.

This isn't unique to "favicon.ico". The RISK is really:

- * people are unintentionally exposing access logs on their web sites,
 exposing user information and possible passwords.
- * hackers can easily find vulnerable systems not by scanning the site itself
 (which can be detected by intrusion detection systems), but by searching a
 3rd party like AltaVista.

Robert Graham
CTO, Network ICE
<http://www.networkice.com/advice>

⚡ Leap year 2000 and C

Mark Brader <msbrader@interlog.com>
Sat, 17 Apr 1999 02:03:08 -0400 (EDT)

I missed the following when it came up in comp.lang.c.moderated three months ago, but I think it's worth repeating here. In C, a time and date represented by a single number (called a `time_t`) can be split into components (year, month, day, hour, etc.) by either of a pair of library functions, `gmtime()` and `localtime()`, which differ only as to the time zone they use (if that information is available).

Two of the components have unusual representations, for

convenience in particular uses. The month goes from January = 0 to December = 11, which is handy for indexing an array of month names. And the year is represented with 1900 subtracted from it, a system which in pre-Y2K-conscious days must have seemed as though it gave a convenient way of obtaining a "printable form" of a year. Note that it does NOT simply reduce the year to two digits: 1999 is 99, but 2000 is 100, not 0.

Okay, now the bug. Dennis Ritchie posted this:

```
# Until some months ago Plan 9 had an amusing bug: its gmtime
routine
# did not believe that 2000 was a leap year. The code in the
routine
# had the correct test with 4, 100, 400 (we looked very hard at
it).
#
# It turns out that the "year number" being tested was year-
1900,
# not year!
```

And Peter Seebach added this follow-up:

```
| Curiously, BSD/OS had exactly the same problem earlier this
year.
| It's probably going to pop up all over - because no one's
Unix-like
| implementations were adequately tested in 1900, when they
would
| have incorrectly identified the year as a leap year.
```

Since all C implementations since the standard came out are required to include `gmtime()` and `localtime()`, they could also be subject to the same bug, whether on UNIX or not. Note that such a bug could affect dates for some considerable time after 2000-02-29 itself, depending on exactly how the functions are implemented.

Of course, if the implementation got it right, this is a non-issue.

But we see above that there are two that didn't...

Mark Brader, Toronto msbrader@interlog.com

✶ Risks of April foolery

Pete Mellor <pm@csr.city.ac.uk>

Sat, 17 Apr 1999 23:43:24 +0100 (BST)

This is not really computer related, but have a laugh!

Having had experience of two computer April 1st jokes that were taken seriously, I was amused to hear an item on the "Today" programme on BBC Radio 4 on the morning of April the 1st. This concerned a new Euro-anthem which would replace all of the European national anthems. It had been written in German and was sung (very well) by a choir from a German school in London. The tune was the "Ode to Joy" theme from Beethoven's 9th.

The following day, the newsreaders came clean. Yes, it was a joke (although the EU gets up to such daft stuff that the listeners could have been forgiven for believing it).

One particularly eminent listener was apparently impressed by it. The programme received a request for further information from Buckingham Palace, allegedly originating from Prince Charles' staff!

Pete Mellor, Centre for Software Reliability, City University,
London
p.mellor@csr.city.ac.uk

🔥 GUIDs and Melissa

"Robert David Graham" <rob_ni99@netice.com>

Fri, 16 Apr 1999 20:21:06 -0700

> Incidentally, there is confusion among the various news reports of
> Melissa as to exactly when and how the GUID entered into the
> identification of the perpetrator. Can anyone who really knows
> enlighten us? PGN

If you open the Melissa document in BINARY mode (not in Word!), you can see the following string:

```
PID_GUID {572858EA-36DD-11D2-885F-004033E0078E}
```

The underlying issue is very complex. Microsoft assigns a "Globally Unique Identifier" to every object it can get its hands on, including your local machine and user account. They are all over Windows; you see them everywhere.

Well, how do you create a GUID? How do you ensure that it is truly unique in all the world? Microsoft combines timestamp, random number generator, and other unique identifiers in order to come up with the GUID. In particular, all Ethernet adapters come with a unique 48 bit serial number. The first 24-bits are assigned to each company that sells adapters, and the second 24-bits are assigned by the company itself. This prevents two adapters from having the same Ethernet address on the same LAN (RISK note: some vendors assign duplicate addresses either because of mistakes or just because they

don't care, but for this purpose, we can assume it to be unique).

The Ethernet address is the last 48 bit of the GUID. The creator the Melissa document has the Ethernet address 004033E0078E. Look that up in a database, and you see the manufacturer was "Addtron Technologies" owns the address block "004033xxxxxx". In theory, you might be able to look at Addtron's records, and pin point things like which distributor the card was shipped to, then get those records and see who might have bought an Addtron card with credit cards.

Moreover, there is more fun. You can ask for a Windows-machine's MAC address using a "NetBIOS NodeStatus Query". This means that you can scan the Internet looking for this MAC address. You need to send around 4-billion packets, but it might work.

Many companies maintain virus databases; you simply look through those databases and see which viruses have the same GUID. You build up a profile of the virus writer, because they tend to put their names in them. In this manner, they found the GUID matched up with many viruses created by somebody named "VicodinES".

The problem is that all of this is circumstantial. Virus writers tend to grab existing viruses, then modify them to do new things. That was clearly done in the Melissa case, as it is similar to many other viruses with the one change that it e-mails itself around.

The real way they caught the guy is that AOL keeps records, and

found a certain IP-address/timestamp combination. The feds then tracked that down to the ISP, which keeps user-accounts/caller-id/IP-address/timestamp combinations in its database. They then put it together and find the guy. The found the guy's computer in the dumpster, it is unclear whether they've checked the Ethernet card.

Robert Graham, CTO, Network ICE

✦ Phone company says keep your PIN on your calling card

<DavidG3276@aol.com>

Sun, 18 Apr 1999 18:45:38 EDT

As readers are well aware, it is simply good sense to not keep passwords where someone could take advantage of them. Imagine my surprise when a major U.S. telephone company sent us a new calling card along with stickers which listed our calling card and PIN numbers. We were to place these small stickers on the back of the card to make sure that we did not forget either number. How helpful--not just for us, but for any thief who might pick my pocket. Plus, imagine the fun someone could have if they had stolen this letter from our mailbox.

Dave Graf <DavidG3276@AOL.COM>

✦ Re: Mainframe viruses (Schaffer, [RISKS-20.30](#))

Julian Thomas <jt5555@epix.net>

Fri, 16 Apr 1999 19:01:25 -0400

>If a computer has an integrated word processor in its mail software, then
>it very well might not take supervisor privileges for a word processor
>macro to send mail. I think this was the source of the PROFS vulnerability.

Not exactly. IIRC the program was called CHRISTMA EXEC that came in a message that said something to the effect of "Don't worry, just run this". It then proceeded to send itself to everyone in the recipient's address list. It wasn't exclusive to PROFS - also affected users of NOTE.

No integrated word processor, and none of those on VM had anything like the startup macros of word, excel, etc.

Julian Thomas: jt 5555 at epix dot net <http://home.epix.net/~jt>
remove numerics for e-mail

✶ E-mail and communications history (Re: RISKS-25,28)

<dmr@plan9.bell-labs.com>

Fri, 2 Apr 1999 01:18:09 -0500

The recently published "The Victorian Internet" by Standage (Walker, 1998) is not technically deep but has interesting parts, and in particular does discuss the fraternity of telegraphers (earliest chat groups?) and has some discussion of security issues that arose even in the 1800s. No computers

involved, but some of today's issues arose then.

The older "The Early History of Data Networks" by Holzmann and Pehrson (IEEE Computer Society Press, 1995) is more scholarly and includes much more of the earlier history, in particular about the remarkable story of the optical telegraph networks that developed in Europe during the early 19th century.

Link-layer protocols and encoding were important even in 1800.

Disclaimer:

Holzmann is a close colleague, so this is a plug. Anti-disclaimer: the on-line booksellers differ about its availability.

Dennis Ritchie

🔥 REVIEW: "Hacker Proof", Lars Klander

"Rob Slade" <rslade@sprint.ca>

Tue, 6 Apr 1999 08:33:42 -0800

BKHKRPRF.RVW 990228

"Hacker Proof", Lars Klander, 1997, 1-884133-55-X, U\$54.95/C\$74.95

%A Lars Klander lklander@jamsa.com

%C 2975 S. Rainbow Blvd., Suite 1, Las Vegas, NV 89102

%D 1997

%G 1-884133-55-X

%I Jamsa Press/Gulf Publishing Co.

%O U\$54.95/C\$74.95 800-432-4112 fax 713-525-4670

starksm@gulfpub.com

%P 660 p. + CD-ROM

%T "Hacker Proof: The Ultimate Guide to Network Security"

There is a great deal of information on security contained within this

book. Unfortunately, it is presented without a cohesive framework.

The overall impression is good. A lot of the forms that would make up a useful work are followed, such as a summary (rather ironically, in view of the scattered nature of the text, called "Putting It All Together") and a set of resources at the end of every chapter. The author seems to be easily distracted, continually jumping to the next, more sensational, topic.

Although not divided into parts, the contents do have some logical divisions. Initially, we are presented with what seems to be intended as background material, although the scattergun approach leaves all of the synthesis up to the reader. Chapter one is a rather unfocussed introduction, talking as much about Internet technologies as about security. Errors are rather common, ranging from chunks missing out of sentences to figures with no cutlines to security weaknesses that are essentially duplicates of each other to mailing lists that haven't distributed material for years (with contact addresses that are even older). Theoretically the networking concepts and details in chapter two might aid in understanding system vulnerabilities, but in the fact of the book they do not seem to be used effectively. The discussion of firewalls does not provide sufficient information about either the needs, weaknesses, or possible inconveniences of the different types in chapter three. The material on encryption, in chapter four, mentions a number of the currently important standards, but the

explanations are so flawed that the chapter could not be used to inform a decision on the strength or use of a cryptographic system.

Material on the use of digital signatures is fairly short, and the remainder of chapter five rehashes, with really expanding, old ground.

Another section tries to delve into more networking protocols. Chapter six, on HTTP (HyperText Transfer Protocol), is somewhat disjointed, and, again, fails to seriously examine the security implications. S-HTTP (Secure HyperText Transfer Protocol), in chapter seven, deals mostly with packets and commands, although it does have some limited discussion of function. The Secure Socket Layer (SSL) seems to look primarily at arcana rather than use.

Chapter nine looks at a few common forms of attack, but presents information somewhat at random. Kerberos is reasonably well described in chapter ten. Some types of electronic commerce technology are mentioned in chapter eleven. There is an extremely limited look at auditing in chapter twelve, first for UNIX and then for NT. A very rough look at security issues within the Java programming language makes up chapter thirteen. Chapter fourteen's look at viruses has good basic explanations, but is unreliable in practice.

The remaining chapters generally look at security for specific systems. Chapters fifteen to seventeen very quickly talk about individual security functions in NT, NetWare, and UNIX, but fail to analyze, for example, the effective rights granted by combinations of the different privilege granting mechanisms. SATAN (System Administrator's Tool for Analyzing Networks) for UNIX and Kane Security Analyst for NT get quick overviews in chapter eighteen. Chapter nineteen presents a number of security vulnerabilities

with
the Netscape and particularly the Internet Explorer Web
browsers. CGI
(Common Gateway Interface) form weaknesses are discussed in
chapter
twenty, but with so many different languages that the ultimate
advice
is simply don't make a mistake when programming.

The final chapter is a reasonable look at security policies.
However,
with some many items missing from the background provided, the
chance
of producing a good policy at this point is relatively small.

As with "Maximum Security" (cf. BKMAXSEC.RVW), this book
attempts to
cover the enormous field of security by throwing out as many
bits as
possible. Therefore large holes are apparent in the coverage.
In
addition, the book lacks an overall framework that could be used
to
build a security structure and point the way to vulnerabilities
that
were not addressed. For those who already are well comfortable
with
security as a concept, this volume does have a lot of references
that
might be of use. For those new to the topic, it is not reliable
enough to start with.

copyright Robert M. Slade, 1999 BKHKRPRF.RVW 990228
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

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



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 32

Tuesday 20 April 1999

Contents

- [Airbus Autopilot Failure?](#)
[Chuck Weinstock](#)
- [Another old-fashioned bug comes back to byte](#)
[Jeremy Epstein](#)
- [Risks of running a PKI](#)
[Steve Bellovin](#)
- [New paper on Simulating Cyber Attacks, Defenses, and Consequences](#)
[Fred Cohen](#)
- [Re: Ghost trains](#)
[Peter Campbell Smith](#)
- [Re: GUIDs and Melissa](#)
[David M. Chess](#)
[JDean](#)
[Nick Brown](#)
[Russ Cooper](#)
- [Re: Mainframe viruses](#)
[David M. Chess](#)
[Otto Stolz](#)
- [Re: Microsoft reschedules Memorial Day](#)
[Bernard Sufrin](#)

- [Re: Overzealous applications](#)
[Mark Brader](#)
 - [Re: Overzealous criticism](#)
[Peter da Silva](#)
 - [Calendar problem with old Calvin and Hobbes comics strips](#)
[Michael Cook](#)
 - [AT&T PINs](#)
[e](#)
 - [Ameritech calling card ready to use!](#)
[Nathan Brindle](#)
 - [High-Integrity System Specification and Design book](#)
[Jonathan Bowen](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ **Airbus Autopilot Failure?**

Chuck Weinstock <weinstock@sei.cmu.edu>

Mon, 19 Apr 1999 16:49:28 -0400

I imagine it is too soon to know for sure whether it was an autopilot failure. We've seen enough finger pointing in other incidents for us not to believe the first reports without some additional evidence.
Chuck

On 19 Apr 1999, an Air India Airbus 320 en route from Singapore to Bombay via New Delhi had apparent had an autopilot failure at 27,000 feet, resulting in a dive that injured three crew members (two seriously) and an infant. The pilot was able to regain control, and manually flew the jet to Bombay. [Source: AFP, 19 Apr 1999; PGN-ed]

🔥 Another old-fashioned bug comes back to byte

"Epstein, Jeremy" <Jeremy_Epstein@NAI.com>

Mon, 19 Apr 1999 14:11:50 -0700

Wired reports in "'EBayla' Bug Strikes eBay" (see <http://www.wired.com/news/news/technology/story/19207.html>) that eBay users can enter an HTML description of the item being auctioned. However, the script provided by the seller can also include Javascript, thus allowing the seller to create a fairly simple web page that, when accessed by the unsuspecting bidder, can capture the bidder's eBay username and password and send it to the bidder (or anyone else).

This is a new version of an old bug: if you allow users to specify input that can be used by others, make sure there's enough filtering that it can't be harmful.

Perhaps the scariest part was the reaction from eBay, as reported by Wired:

"Ebay's senior director of corporate communications characterized the hole as an 'occasional byproduct' of the service's user-focused design." eBay downplayed the severity of the exploit, noting that "If somebody had indeed used your password as well as your username and started bidding on a bunch of items, you'd be the first person to be contacted by eBay through e-mail, and we'd be able to backtrack on that to make sure that we could take care of that situation."

Gee thanks. After it happens, you'll let me know I just bought a velvet

Elvis and a set of matching pink lawn flamingos :-)

✂ Risks of running a PKI

Steve Bellovin <smb@research.att.com>

Mon, 19 Apr 1999 10:42:02 -0400

There are many problems involved in setting up a robust public-key infrastructure. An oft-overlooked issue is bookkeeping -- just keeping track of what has been done. Today, even the most sophisticated companies can't get this right.

The other day, my daughter clicked on "Windows 98 Update" on her machine.

Up popped the usual request to accept an ActiveX control. When she clicked on "Microsoft", a nice red "X" showed up -- the certificate had expired.

Now, this has to be one of the most important non-root certificates in existence, since it controls updates to an extremely popular platform. And it is owned by one of the most technological companies in existence. And it was mishandled.

This isn't the first occurrence of this problem -- I reported similar incidents to Microsoft at least 9 months ago. And the problem isn't that the code had been tampered with, simply that some certificate in the chain had expired. But the administrative issues -- keeping track of all of the certificates -- are formidable.

There are also human factors issues here. The initial pop-up

box doesn't indicate that there may be a problem. The secondary pop-up doesn't give the user any guidance on how to evaluate the seriousness of the issue -- should the control be accepted or not. And there was timezone and notational confusion -- this occurred late on April 16, the day the certificate expired -- if the certificate expired at midnight UTC, it was indeed invalid; if it expired at midnight Eastern time, where we were, or Pacific time, where Microsoft is, the checking code is buggy. There was also the usual question of 12am/12pm vs. noon or midnight.

My point here is not to pick on Microsoft. Rather, I'm asserting that the real difficulties in utilizing a PKI aren't solved by things like X.509 or SPKI; rather, there are serious generic issues involving keeping track of certificates and presenting the information to users in a useful form.

🔥 New paper on Simulating Cyber Attacks, Defenses, and Consequences

Fred Cohen <fc@all.net>
Tue, 20 Apr 1999 10:33:14 -0700 (PDT)

This morning, I posted a new paper to the all.net Web site that I think you might be very interested in. It will soon appear in print as an invited paper in "Computers and Security", it will be briefly covered in one of my short presentations at the IEEE Oakland conference, and it will

be given in
its entirety at the upcoming CSI conference. The paper is
titled:

"Simulating Cyber Attacks, Defenses, and Consequences"

and it can be found at the all.net web site under:

Feature Articles: InfoSec Baseline Studies

I think that this is one of the most interesting papers I have
written in
the last two years, and I ask that those of you who are
interested in such
things take the time to read and comment on it. I thank you for
your time.

FC

Fred Cohen & Associates: <http://all.net> - fc@all.net - tel/
fax:925-454-0171

[Fred's disclaimer omitted, distinguishing his FC&A and Sandia
roles. PGN]

✉ Re: Ghost trains (PGN, [RISKS-20.31](#))

"Campbell Smith, Peter" <CampbellP@logica.com>

Tue, 20 Apr 1999 14:23:13 +0100

PGN reported that recently a ghost train appeared in the BART
(San Francisco
metro) computers and he was surprised that 567 such incidents
occurred in a
two-year period.

Very many rail systems, BART included, use track circuits to
detect trains -
ie they rely on the train itself making an electrical connection
between the
two running rails. There are other detection methods used

instead of or in conjunction with track circuits, but track circuits have been used for decades, are acceptably reliable in hostile environments and are generally accepted as safe. If they fail, they are much more likely to falsely report a train than falsely report the track as vacant.

One snag with track circuits is that they can only localise a train to somewhere within a stretch of track. To track trains reliably in a busy rail system like BART it is necessary to apply some additional heuristics, starting with the first law of train control - trains cannot be created or destroyed. This can still leave ambiguities: for example if three trains occupy adjacent track sections and then a gap opens up, is it behind or in front of the middle train? BART and other systems have a hierarchy of automatic algorithms followed by manual procedures and operating rules to overcome these sorts of problems, but however this is done there is always the possibility of ghost trains - ie track sections which appear to be occupied but which cannot be associated with a known train.

There are two main causes of ghost trains: failure to track correctly a real train - in which case the controller (human or computer) needs some independent corroboration that the train is in the section, and faulty track circuits, when the controller similarly needs corroboration that the section is indeed vacant. All rail systems, BART included, have operating procedures which allow trains to continue running, subject to certain rules,

when track circuits fail.

Computerised control systems however have their limits and if a series of track circuits fails, especially in a congested area such as the one reported, the best option is to switch to manual control. The reason for this is that the only safe way to operate automatically would be to allow only one train at a time into the 'blind' section and wait for it to reappear at the other side before letting the next one in. Under manual control however trains can be made to go very slowly, to be driven with the driver in radio contact with control, or to operate with visual signals or even flagmen.

So in short, it isn't very surprising, at least to those who design train control systems, that ghost trains occur so often. They have been foreseen by those that built the system and it has been designed to operate safely, if not perhaps very rapidly, in their presence.

Peter Campbell Smith

⚡ Re: GUIDs and Melissa (PGN, [RISKS-20.31](#))

David M. Chess <chess@us.ibm.com>

Mon, 19 Apr 1999 11:34:08 -0400

> [Incidentally, there is confusion among the various news reports of
> Melissa as to exactly when and how the GUID entered into the
> identification of the perpetrator. Can anyone who really knows

> enlighten us? PGN]

Well, I won't claim to really really know, but I may know as much as anyone else who's free to reveal. From what I can tell, the GUID in the original LIST.DOC was the same as the GUID in a document used to distribute an earlier virus (by "Vcodin ES"), and the same as the GUID in an even earlier document used to distribute an even earlier virus by someone with an even sillier "handle". Since the GUID isn't updated when an existing module is modified, it seems likely that this provides evidence only that virus writers tend to build on earlier viruses; something everyone already knew. It could provide evidence against the author of Melissa only rather indirectly; if for instance a number of documents were found containing early drafts of Melissa, or showing the progressive modification of the earlier Vcodin ES virus into Melissa, the continuity of GUIDs would help round out the story. But it is likely not the case that the GUID directly implicates the author; the GUID of the original Melissa LIST.DOC is probably not the same as the GUID placed in brand-new documents created on the virus author's system.

DC

[The reason for my original note that Dave has reproduced (above) was my suspicion that media reportage falsely implied that the GUID explicitly implicated the person arrested. But remember, digital evidence should always be considered suspect, especially with sloppy system

security and
sloppy administration, but even in the best of circumstances.
PGN]

✉ Re: GUIDs and Melissa (Graham, [RISKS-20.31](#))

<jdean1@nomvs.lsumc.edu>

19 Apr 99 06:36:46 -0500

> If you open the Melissa document in BINARY mode (not in
Word!), you can see
> the following string:
>
> PID_GUID {572858EA-36DD-11D2-885F-004033E0078E}

Assuming this conforms to Internet Draft
<draft-leach-uuids-guids-0.txt>, the date portion decodes to
8/18/1998 20:52:22.510 UTC -- long before Melissa appeared.
(<ftp://colbleep.ocs.lsumc.edu/pub/utility/win95/decoguid.zip>
contains my program to decode GUIDs).

✉ Re: GUIDs and Melissa (Graham, [RISKS-20.31](#))

BROWN Nick <Nick.BROWN@coe.fr>

Mon, 19 Apr 1999 12:52:25 +0200

The NIC address which is placed in the GUID, is not obtained
directly from
the network card's hardware. It is obtained from the driver.
And on NT at
least (and I imagine on 95/98), you can change this. On NT it's
at
(assuming a NIC of type <card>):
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\<<card>1
\Parameters

Add a string named "NetworkAddress" containing 12 hex digits, reboot, and away you go.

Of course, this is hugely powerful. I get my colleague's NIC address with ping and arp. Then I disconnect my PC from the network (to avoid conflicts), change my NIC address, create my Word document saying "the boss sucks", and leave the document lying around... (I'm assuming that if I just edit the document with Notepad to change the GUID, something might break in a checksum or something, but even that isn't clear). When the network administrator is called in to help in the witch-hunt, he'll find a smoking gun leading to my colleague's PC... in the office which he keeps locked at all times...

If you have a NIC but you're not currently on a LAN, I recommend changing your NIC address to 4675636B4D24, but you can use this mechanism to send any 6-character ASCII message you want...

Nick Brown, Strasbourg, France

✉ RE: GUIDs and Melissa (Graham, [RISKS-20.31](#))

Russ <Russ.Cooper@rc.on.ca>
Tue, 20 Apr 1999 01:27:53 -0400

Robert Graham made some reasonable observations about GUIDs in the [20.31](#) digest, I would add...

1. If the machine does not have an Ethernet adapter, but say,

has a modem instead (or no adapter), the MAC address component of the machine's base GUID is randomly generated at OS install time. It then appears to be re-used by anything that generates a GUID. There is no indication that it attempts to exclude adapter vendor assigned address space when generating this random value, meaning it may well duplicate a *real* MAC address.

2. GUIDs are based on the owner of the document. So in the case of virus databases and such, they would have to know they have a source document, not some document which had been infected, to know they had the original. In the case of Melissa, because it spread so quickly, the parties (Richard Smith of Pharlap et al) believed they had the original from the newsgroups it first appeared in. While its possible, there's no way to prove it.

3. GUIDs don't identify the person who keyed the document, only the machine on which they were keyed. Anyone fearing repercussions from the circumstantial evidence merely has to do a fresh install of their OS to replace their GUID. In today's computing environment, it actually makes more sense to simply take the drive out to the road and run over it with your car a few times and throw it off a bridge, then for \$150 replace it with a new one (and during the new OS install generate an entirely new GUID). Cutting and pasting the contents of one document (from one machine) to another (from another OS install or different machine) allows the contents to obtain a new GUID (or the GUID of someone

you
want to implicate if you have any other document from them).

While the press picked up on the GUID issue quickly (largely due to recent discussions about it and Richard's penchant for talking with the media), fact is if it were ever introduced and accepted as any sort of evidence we'd all be in for some bad times.

I remember the furor that was caused when an email, purported to be from the former Premier of Ontario Bob Ray, was put into the hands of the media. He was blasted for its contents, when in fact its author was merely identified by a FROM: address in an SMTP message. GUIDs in an MS document represent about the same level of assurance as to who the author was.

The obvious risk is that we need to ensure we're relying on reliable information as evidence of anything, as I'm sure Fred Cohen would agree...;-]

Russ - NTBugtraq moderator <http://ntbugtraq.ntadvice.com>

✶ Re: Mainframe viruses (Kabay, [RISKS-20.31](#))

<chess@us.ibm.com>

Mon, 19 Apr 1999 11:50:54 -0400

>The Christmas Tree "virus" affected VM systems some 10+ years ago. (IIRC
>it really affected PROFS.) I think it is reasonably comparable to Melissa.

In fact CHRISTMA EXEC worm (back in 1987) was a rather generic VM/CMS mail exploiter; it didn't require PROFS (one popular CMS mail client), nor as I recall did it specifically target the PROFS address book when looking for addresses to spam itself to. The similarities to Melissa are many: victims would receive a CHRISTMA EXEC in the mail from someone they knew (someone whose address book, roughly, they were in), and have to perform an explicit action (receive and run it) to have the worm actually execute.

>> Microsoft engineers decided to dispense with a security kernel ...

>If a computer has an integrated word processor in its mail software, then it

>very well might not take supervisor privileges for a word processor macro to

>send mail. I think this was the source of the PROFS vulnerability.

This is a very good point. Of course it does not require supervisor privileges either to send e-mail or to alter one's own documents. In general, viruses do not need to violate access controls or obtain root privilege or alter the operating system in order to spread. I think in the original piece Mr. Kabay overemphasizes the lack of security in DOS-heritage systems when thinking about the causes of virus vulnerabilities. In fact, until the rise of network connectivity, PC security was very very strong: you, sitting at your PC over there, would have a much *harder* time altering files on my PC over here than the typical multi-user-system user would have altering files belonging to someone else on the same system.

Since viruses spread via *authorized* communication channels (programs and documents that I intentionally share, or email that I am permitted to send), preventing programs from exercising unauthorized features isn't terribly relevant. Certainly there are things that current office systems could do better, security-wise, such as recognizing that a program or documents is from an untrusted source and limiting its function appropriately, but it's not realistic to imply that if only Microsoft had put a security kernel into Windows, viruses would never have become a problem. Whenever people use general-purpose programmable systems, and intentionally share programs and active content, viruses will continue to be a threat we must guard against; simply applying traditional access-control security to a system does not render viruses on that system either impossible or harmless.

DC

✶ CHRISTMA EXEC (was: Mainframe virus; [RISKS 20.30](#) and [20.31](#))

Otto Stolz <Otto.Stolz@uni-konstanz.de>
Tue, 20 Apr 1999 10:38:22 -0600

Some corrections are due (this is not "IIRC", as the recent contributions:
I've been there, seen it, even kept records).

On Fri, 9 Apr 1999 21:27:19 -0400 (EDT), hes@unity.ncsu.edu said:
> The Christmas Tree "virus" affected VM systems some 10+ years

ago.

> (IIRC it really affected PROFS.)

It propagated only on VM/CMS systems, but it affected the whole EARN/Bitnet/Netnorth and IBM's internal network Vnet, due to network overloading, from 1987-12-09 through 1987-12-14th. PROFS was not needed (cf. infra).

> I think it is reasonably comparable to Melissa.

Melissa propagates in two ways, both as a Word Macro Virus, and by sending mail through a particular e-mail user agent. In contrast, CHRISTMA EXEC was not a virus, and exploited CMS's SENDFILE command (a predecessor of FTP); PROFS, a mail service, was not used, at all. This type of code was then dubbed "Rabbit".

On Fri, 16 Apr 1999 19:01:25 -0400, jt5555@epix.net (Julian Thomas) said:

> IIRC the program was called CHRISTMA EXEC that came in a message that

> said something to the effect of "Don't worry, just run this".

Not quite so. It came as a bare EXEC file (akin to a .Bat file in the PC world, or to a shell script, in the Unix world), i. e. as a source file anybody could read (and everybody was supposed to understand :-)).

It contained, after several screens full of rather boring REXX statements of the sort "display so-and-so many blanks and then so-and-so many asterisks...", a screen-sized comment block saying "Browsing a dull program like this one is no fun; just type CHRISTMAS to run it" or something to this effect. Actually, the addressee had to explicitly RECEIVE the

file (i.e.,
move it from the system spool area to a local disk) before
typing CHRISTMA
would work. The blanks and asterisks would, of course, generate
an ASCII-art
image of a Christmas tree, on the user's screen.

> It then proceeded to send itself to everyone in the
recipient's address
> list. It wasn't exclusive to PROFS - also affected users of
NOTE.

It harvested the addresses from two files: an audit trail of
former file
transfers (including e-mail sent and received), and the user's
personal
address book. Both were used by the CMS commands NOTE and
SENDFILE; I do not
know, whether PROFS used these same files.

The incident was discussed in RISKS: issues [5.72](#), [5.74](#), and
[5.79](#), carry only
folklore and open questions; in issue [5.80](#), item1, Ross Patterson
comprehensively discusses CHRISTMA EXEC; issues [5.81](#) through [6.1](#)
carry minor additions,
and even more folklore (viz. a press item meant as a deterrent
example of journalists not understanding the issues they are
reporting
about); issues [6.1](#) through [6.7](#) discuss whether source-code
availability
implies any security.

Five years later, CHRISTMA EXEC was discussed in Virus-L, issues
5-176
through 5-206 (and I had to correct, in issue 5-178, the same
errors now
re-told in RISKS); to get the archive files of this latter
discussion, send
e-mail to listproc@Lehigh.EDU
containing the following lines:
search Virus-L -all "CHRISTMA EXEC"
get virus-l/Digests 5-176

get virus-1/Digests 5-178
(and so on; use the results of the search command mailed to you).

CHRISTMA EXEC "inspired" several epigones [*], who later
produced the
Rama, ZebraTell, Game2, and other VM rabbits [*].

Otto Stolz

[* Must have been epigonadotrophic. PGN]

🔥 Re: Microsoft reschedules Memorial Day

<bernard.sufrin@comlab.ox.ac.uk>

Mon, 19 Apr 1999 11:56:36 +0100

Outlook 98's view of the dates of at least two of the UK bank
holidays
this year is also wrong by a week.

🔥 Re: Overzealous applications (Cargill, [Risks-20.31](#))

Mark Brader <msbrader@interlog.com>

Mon, 19 Apr 1999 03:23:33 -0400 (EDT)

> Thus if you enter 2/4/99, it will be interpreted as 2 April 99
> in the
> UK, 4 Feb 99 in the US, etc. Fine so far, but what if you
> enter an
> invalid date, such as 29/2/02? ... in fact, Access quietly
> accepts this
> as a valid date - 29 Feb 2002!! The trouble seems to be that
> Access
> tries too zealously to find a 'correct' interpretation, so if
> dd/mm/yy
> (or mm/dd/yy) doesn't work, then it tries yy/mm/dd.

If that's the reason, I hope it interprets it as 2 Feb 2029, not 29 Feb 2002!!

Mark Brader, Toronto, msbrader@interlog.com

✉ Re: Overzealous criticism (Re: Cargill, [RISKS-20.31](#))

Peter da Silva <peter@baileynm.com>

19 Apr 1999 16:36:32 GMT

>Fine so far, but what if you enter an invalid date, such as 29/2/02?

I assume you mean something like 2/2/29, because I would expect 29/2/02 to be accepted as 29 Feb 2002. Or did it come out as 2 Feb 1929?

> The trouble seems to be that Access tries too zealously to find a
> 'correct' interpretation, so if dd/mm/yy (or mm/dd/yy) doesn't work, then
> it tries yy/mm/dd.

Which is the normal date format in Japan.

> Of course, the problem goes away if you require users to enter four-digit
> years, but it is still unwarrantedly aggressive behaviour.

Much as I like to lob bombs at Microsoft, I can't legitimately fault them for this. It's the social issues behind the Year 2000 problem that caught them up.

Peter da Silva <peter@baileynm.com>

⚡ Calendar problem with old Calvin and Hobbes comics strips

Michael Cook <mlcook@cca.rockwell.com>

Tue, 20 Apr 1999 12:56:21 -0500

The "Calvin and Hobbes" comic strip web site has a calendar problem!

Universal Press Syndicate is re-running old C&H comic strips. Each day they run the strip from that date 11 years ago.

Another example of calendar problems in general, and a pre-Y2K Y2K problem!

The note on the C&H web pages:

Calvin is back! Each day we are reissuing an original Calvin and Hobbes

strip, 11 years after it was first published. Start your adventure with

the first Calvin and Hobbes Strip, published November 18, 1985. Please

note: 1988 was a leap year, therefore, Sunday comics will appear on

Saturday through February 2000.

<http://www.calvinandhobbes.com/strips/88/04/ch880417.html>

[change date to wherever you want to start. ^^^^^^

But the 2-digit year field is not a problem here! PGN]

⚡ AT&T PINs (Re: [RISKS-20.31](#))

e <erisks@gmx.net>

Mon, 19 Apr 1999 10:57:45 -0400

AT&T does this all the time. my so-called PIN is actually

printed onto the
card as the last four digits of the long number.

I can only assume that telcos don't really care if "cards" (all
you need is
the n-digit number that's printed on it) are used by others, as
long as
someone pays the bill. And I admit that I never worried too much
about it
because my employer does that -- I would not accept this method
for
something i was paying for personally.

✶ Ameritech calling card ready to use! (Re: [RISKS-20.31](#))

Nathan Brindle <nbrindle@netdirect.net>

Mon, 19 Apr 1999 17:16:24 -0500

I received a new calling card from Ameritech in today's mail.
Conveniently
enough they placed two little peel-off stickers--one with my
telephone
number, the other with my PIN--right next to the calling card,
on the
folder it came in. I'm sure they consider this to be less RISKy
than
actually printing the numbers on the card for me. Awfully nice
of them,
don't you think? :)

This is the kind of thing that makes me glad my mailbox has a
lock :)

Nathan

✶ High-Integrity System Specification and Design book

Jonathan Bowen <jpb@csres.cs.reading.ac.uk>

Tue, 20 Apr 1999 14:13:48 +0100 (BST)

The following book may be of interest to RISKS readers. It provides an introduction to computer-based system specification and design, paying particular attention to structured and formal methods, method integration, concurrency and safety-critical systems. The book consists of both original material and reprints of classic papers in the field of system specification and design.

J.P. Bowen and M.G. Hinchey. High-Integrity System Specification and Design. Springer-Verlag, London, FACIT series, April 1999.

xviii+701 pages, 65 UK pounds. ISBN 3-540-76226-4.

Paper authors include Brooks, Craigen, Harel, Hoare, Lamport and Leveson.

For further on-line information, see:

URL: <http://www.fmse.cs.reading.ac.uk/hissd/>

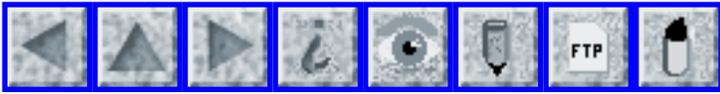
This includes a full list of papers and an electronic copy of the preface and table of contents.

Jonathan Bowen, The University of Reading, Dept of Computer Science

Whiteknights, PO Box 225, Reading, Berks RG6 6AY, England

Tel: +44-118-931-6544 (direct) -8611 (enquiries) Fax: +44-118-975-1994

Email: J.P.Bowen@reading.ac.uk URL: <http://www.cs.rdg.ac.uk/people/jpb/>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 33

Saturday 24 April 1999

Contents

- [Expert warns of safety glitch in shopping carts](#)
[Keith A Rhodes](#)
- [The CIH virus will strike Monday, April 26!](#)
[Satomi Hamamoto](#)
- [eBayla virus](#)
[Jeff E. Kinzli via Dave Farber](#)
- [Use a cable modem, go to jail](#)
[Lenny Foner](#)
- [Risks of over-helpful software](#)
[Jim Horning](#)
- [More on running a PKI](#)
[Steven M. Bellovin](#)
- [CompuServe responds to password-solicitation fraud](#)
[Mich Kabay](#)
- ["In order to make it easier for you"](#)
[T Bruce Tober](#)
- [Melissa, GUIDs, and VicodinES](#)
[Richard M. Smith](#)
- [Re: GUIDs and Melissa](#)
[Jiri Baum](#)

● [REVIEW: "Y2K Risk Management", Goldberg/Davis/Pegalis](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ Expert warns of safety glitch in shopping carts

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

Fri, 23 Apr 1999 14:52:05 -0500

Joe Harris of the Seattle-area Blarg! Online ISP has warned that commonly used ``shopping-cart'' software has a vulnerability that when improperly installed potentially exposes credit-card numbers and other personal information. Harris found over 1000 sites on the Internet with this risk.

The article ends thusly: "When correctly installed, shopping cart software creates a file for confidential information that is inaccessible to

outsiders." Well, maybe? Do you believe in PC security?

[Source: item by

Jeff Wilson, Associated Press, 22 Apr 1999; PGN-ed]

⚡ The CIH virus will strike Monday, April 26!

"Satomi Hamamoto" <toni.hamamoto@sri.com>

Fri, 23 Apr 1999 19:04:49 -0700

[From an internal SRI warning...]

Two variants of the W32.CIH.Spacefiller virus could seriously disable unprotected PCs on Monday, April 26. Introduced in June 1998, variants 1.2

and 1.3 are set to detonate on April 26 and can affect Windows 95 and 98 executable files, bringing about data loss and system crashes. The virus can spread over e-mail when infected executable files are sent as attachments. IBM also recently reported that some Aptiva PCs manufactured in March 1999 are infected with the virus.

To protect yourself against the CIH Virus, and to eliminate it from your system:

Download kill_cih.exe, click here to direct link to the exec file:
http://insider.sri.com/is/antivirus/kill_cih.exe and save it at the

Desktop.

Double click on the file from your desktop.

After running kill_cih.exe, update your Norton AntiVirus virus definitions, using the LiveUpdate feature. To load Norton AntiVirus, go to Start --> Programs --> Norton AntiVirus --> Norton AntiVirus Click on the LiveUpdate button, and choose to update via the Internet.

Then scan your computer using Norton AntiVirus. Remember to select all drives then click on "Scan Now."

For more information, visit Symantec's Kill CIH website:
http://www.symantec.com/avcenter/kill_cih.html

IP: eBayla virus

"Jeff E. Kinzli" <kinzli@cisco.com>
Thu, 22 Apr 1999 17:34:41 -0700

[From Dave Farber <farber@cis.upenn.edu>'s IP list]

From <http://www.tbtf.com/index.html>

..eBayla

Canadian security enthusiast Tom Cervenka, who goes by the handle Blue Adept, has invented a new flavor of virus: he has created an infected eBay auction item [1] that he calls eBayla. The exploit works because eBay allows JavaScript in the member-authored pages describing an item offered for sale. When an eBay member bids on an infected item, his/her username and password are e-mailed to Cervenka. EBay's response [2] to the exploit sets a new low for bone-headedness. Not only does eBay downplay the seriousness of the security hole; not only do they get the technical details of the exploit's workings wrong; but they also make vague threats in Cervenka's direction, because he brought this vulnerability to their attention. EBay deserves to get slapped, hard, by its members -- nothing else will make them rethink their cluelessness. Thanks to Michael Sanders <msanders at confusion dot net> for the prod on this story.

[1]

<http://www.because-we-can.com/ebayla/default.htm>

[2]

<http://www.news.com/News/Item/Textonly/0,25,35321,00.html>

⚡ Use a cable modem, go to jail

Lenny Foner <foner@media.mit.edu>

Fri, 23 Apr 1999 17:26:27 -0400

A harrowing tale of serious criminal prosecution, unstoppable bureaucracies, and the dangers of not wanting to watch cable TV:

<http://members.home.net/maycomp/cablemodem.htm>

✶ Risks of over-helpful software (Re: [RISKS-20.32](#))

Jim Horning <horning@intertrust.com>

Wed, 21 Apr 1999 11:22:55 -0700

Microsoft's mail/calendar/contacts/tasklist program Outlook 98 has what seems like a nifty feature: In addition to hand-constructed filters that you can use to classify/move/delete/flag incoming mail according to its properties, there is a built-in "Junk E-mail" filter, to which one can add easily add new sources of spam as one identifies them (according to one's own private criteria).

Shortly after activating this feature, I had a look at the file of Junk E-mail messages it had shielded me from. To my astonishment, in the midst of the spam, there were a couple of apparently innocent messages from colleagues right here at work, which I rescued. Now I have formed the habit of occasionally scanning the Junk E-mail folder to re-classify any non-junk that lands there. (Of course, the need to do this makes the feature somewhat less valuable.) After fairly diligent searching, I

have concluded
that although one can ADD addresses that will be treated as Junk
sources,
one cannot modify or REMOVE rules that cause messages to be
treated as Junk.

Why am I reporting this to RISKS at this time? Simply because I
discovered
this morning that Outlook 98 had classified [RISKS vol. 20, no.
32](#) as junk,
for reasons that are not obvious to me. I think maybe I'll
deactivate the
feature.

Jim H.

✶ More on running a PKI ([RISKS-20.32](#))

"Steven M. Bellovin" <smb@research.att.com>

Wed, 21 Apr 1999 16:15:23 -0400

Today I decided to upgrade a copy of Netscape Communicator.
That process
also involves certificates. They're not any better -- one of
the packages
downloaded (mBED) was protected by a certificate that expired 21
July 1998.

I also noticed another certificate that expires tomorrow -- I
declined
permission to do that update; I want to see what happens in a
couple of
days.

There are other potential security problems with both update
sequences.
Neither appears to use cryptography to protect the downloaded
code, as
opposed to the installation program -- or, if cryptography is

used, there's no hint of it given to the user. Neither seems to check the expiration date on these certificates. Neither gives any guidance on how to evaluate certificates or CAs, or even that one should do so. Netscape, at least, pops up warnings that the action you're about to take is dangerous -- but a previous box tells you "click grant". Of course, that's all coming from an http page (as is Microsoft's update screen), not an https page, which means that a high-end attacker could substitute its own code and look-alike instructions. The certificate would be wrong, but users don't know to check that.

⚡ CompuServe responds to password-solicitation fraud

Mich Kabay <mkabay@compuserve.com>

Thu, 22 Apr 1999 06:44:08 -0400

I recently received an obviously fraudulent e-mail request claiming to be from CompuServe administration and demanding that I submit my user-ID, password, and full credit-card information. After I forwarded it to CompuServe support I received a response with the following key text:

> There are currently numerous e-mail messages circulating on
> the service claiming to be official CompuServe notices of
> account
> and/or billing problems being sent to members which contain
> a form that is supposed to be filled out and returned by e-mail
> or a termination of the account will occur. It is an attempt
> to steal your credit card and CompuServe account information!

>
> DO NOT respond to this or any similar e-mail!
>
> Instead forward a copy of the complete message by e-mail
> to the CompuServe Internet address actionteam@compuserve.com.

RISKS readers may want to remind naive users of any ISP be warned never to respond to requests to reveal their passwords to anyone at an ISP or indeed, on any network. Even in the rare cases where it would be useful to log into a specific account for problem resolution, any authorized personnel who need access to an account will have the capabilities required to change its password themselves. They do not need to know the user's original password.

M. E. Kabay, PhD, CISSP, Director of Education -- ICSA, Inc.

From: CompuServe, INTERNET:70006.101@compuserve.com
To: [unknown], mkabay
Date: 1999-04-20 14:34
RE: Feedback reply (Ref #1900)

Fr: T.J.
Customer Service Representative

I am writing in response to your question about Password or Credit Card solicitation.

There are currently numerous e-mail messages circulating on the service claiming to be official CompuServe notices of account and/or billing problems being sent to members which contain a form that is supposed to be filled out and returned by e-mail or a termination of the account will occur. It is an attempt to steal your credit card and CompuServe account information!

DO NOT respond to this or any similar e-mail!

Instead forward a copy of the complete message by e-mail to the CompuServe Internet address actionteam@compuserve.com.

IMPORTANT

If you have responded to a message such as this and provided your personal information, CompuServe recommends that you take the following steps to secure your credit card and account information.

1. Contact your credit card company's customer service department and notify them that your information has been compromised.
2. Change your CompuServe password, using the GO PASSWORD command. Your password should not be something that is easily guessed. The best passwords contain letters, numbers, and special characters (like ! or @).
3. Contact CompuServe Customer Service by calling 1-800-848-8990, to resolve any issues which may have arisen as a result of your account being compromised.

Please be assured that CompuServe is taking measures to prevent situations such as this from happening in the future.

If you need further assistance, please write Customer Service again (GO FEEDBACK).

 **"In order to make it easier for you"**

T Bruce Tober <octobersdad@reporters.net>

Sat, 24 Apr 1999 06:57:15 +0100

And this just in from the manager of a list to which I subscribe:

+++++ Forwarded Message +++++
+

Since the migration to the new site, many of you have experienced problems with the login process. In order to make it easier for you, we attempted to create an e-mail with your username and password. However, due to a program error, e-mails were sent to multiple users, disclosing other users' information.

We sincerely apologize for this error and any inconvenience this may have caused. In order to assure you that the site is secure, we will reset everyone's password. A subsequent e-mail will follow with your new unique password. You may keep this password, or once you login you may alter your information by selecting Edit Your Profile from the Main Menu.

Again, we apologize for our mistake and we will correct this as soon as possible. Please continue to visit xDSL.com as your source for DSL information!

Dwayne A. Emerick, Manager of Web Development, TeleChoice, Inc.
TeleChoice...The Experience to Get You There <http://www.telechoice.com>

Bruce Tober, <octobersdad@reporters.net>, <<http://www.crecon.demon.co.uk>>

Birmingham, UK, EU +44-121-242-3832 (mobile - 07979-521-106).
Freelance

✦ Melissa, GUIDs, and VicodinES

"Richard M. Smith" <smiths@tiac.net>

Fri, 23 Apr 1999 18:12:15 -0500

I saw the discussion in comp.risks about the Melissa virus and GUIDs and I wanted to pass along some of the information that Rishi Khan (rishi@udel.com) and myself (smiths@tiac.net) discovered during the week after the virus was released.

First on the issue of the GUID, it turns out the GUID in the Melissa document is identical to the GUID of Word document that carried another Word macro virus named Shiver. The Shiver was created in August 1998 by someone using the alias ALT-F11. Given that the 2 GUIDs are the same, Rishi and I came to the conclusion that the Melissa document was created by copying the Shiver document and replacing the Shiver virus code with the Melissa code. This was confirmed by the fact that the list of Web sites in the two documents are identical and the revision logs in the two files are the same except that the Melissa document has one additional entry.

Because the last edit of the Melissa document occurred only 30 minutes before the virus was posted to the Web, it looks like the Melissa virus was developed in separate document and then combined with the Shiver Web site list at the last minute.

The GUID then in the Melissa document most likely then contains the Ethernet

adapter address of ALT-F11's computer or a computer that he (or she) had access to back in August, 1998.

What's the connection then between David L. Smith, the person alleged to have released the Melissa virus, and VicodinES? It turns out there are many connections because both David Smith and VicodinES posted extensively on the Web and in newsgroups.

One of the more interesting connections was found on the VicodinES Web site.

I was pointed to this Web site a few days after the Melissa virus started spreading by Fredrik Bjork of Sweden. He noticed many similarities between the style of the VicodinES and the Melissa virus author. I was able to download about 10 Word .DOC files from the VicodinES Web site that contained various Word Macro viruses. In 2 or 3 the files I found David L. Smith's name and his initials DLS. In particular, only his name showed up multiple times in the hidden revision log of a VicodinES virus toolkit.

Here is a hex dump from the Word .DOC file from July 1998:

```

12F0:FF FF 12 00 00 00 0D 00 44 00 61 00 76 00 69
00 .....|D.a.v.i.
1300:64 00 20 00 4C 00 20 00 53 00 6D 00 69 00 74 00 d. .
L. .|S.m.i.t.
1310:68 00 23 00 43 00 3A 00 5C 00 57 00 49 00 4E 00 h.#.
C.:.|\.W.I.N.
1320:44 00 4F 00 57 00 53 00 5C 00 44 00 65 00 73 00 D.O.W.
S.|\.D.e.s.
1330:6B 00 74 00 6F 00 70 00 5C 00 43 00 6F 00 6E 00 k.t.o.
p.|\.C.o.n.
1340:76 00 65 00 72 00 74 00 20 00 42 00 65 00 74 00 v.e.r.
t.| .B.e.t.
1350:61 00 2E 00 64 00 6F 00 63 00 0D 00 44 00 61 00 a...d.

```

o.|c...D.a.
1360:76 00 69 00 64 00 20 00 4C 00 20 00 53 00 6D 00 v.i.
d. |L. .S.m.
1370:69 00 74 00 68 00 35 00 43 00 3A 00 5C 00 57 00 i.t.
h.5.|C.:.\.W.
1380:49 00 4E 00 44 00 4F 00 57 00 53 00 5C 00 54 00 I.N.D.
O.|W.S.\.T.
1390:45 00 4D 00 50 00 5C 00 41 00 75 00 74 00 6F 00 E.M.P.
\.|A.u.t.o.
13A0:52 00 65 00 63 00 6F 00 76 00 65 00 72 00 79 00 R.e.c.
o.|v.e.r.y.
13B0:20 00 73 00 61 00 76 00 65 00 20 00 6F 00 66 00 .s.a.
v.|e. .o.f.
13C0:20 00 43 00 6F 00 6E 00 76 00 65 00 72 00 74 00 .C.o.
n.|v.e.r.t.
13D0:20 00 42 00 65 00 74 00 61 00 2E 00 61 00 73 00 .B.e.
t.|a...a.s.
13E0:64 00 0D 00 44 00 61 00 76 00 69 00 64 00 20 00 d...D.
a.|v.i.d. .
13F0:4C 00 20 00 53 00 6D 00 69 00 74 00 68 00 35 00 L. .S.
m.|i.t.h.5.
1400:43 00 3A 00 5C 00 57 00 49 00 4E 00 44 00 4F 00 C.:.\.
W.|I.N.D.O.
1410:57 00 53 00 5C 00 54 00 45 00 4D 00 50 00 5C 00 W.S.\.
T.|E.M.P.\.
1420:41 00 75 00 74 00 6F 00 52 00 65 00 63 00 6F 00 A.u.t.
o.|R.e.c.o.
1430:76 00 65 00 72 00 79 00 20 00 73 00 61 00 76 00 v.e.r.
y.| .s.a.v.
1440:65 00 20 00 6F 00 66 00 20 00 43 00 6F 00 6E 00 e. .o.
f.| .C.o.n.

1B90:00 1E 00 56 00 69 00 63 00 6F 00 64 00 69 00 6E ...V.i.
c|.o.d.i.n
1BA0:00 45 00 53 00 20 00 56 00 42 00 41 00 20 00 53 .E.S. .
V|.B.A. .S
1BB0:00 74 00 72 00 69 00 6E 00 67 00 20 00 43 00 6F .t.r.i.
n|.g. .C.o
1BC0:00 6E 00 76 00 65 00 72 00 74 00 65 00 72 00 00 .n.v.e.
r|.t.e.r..
1BD0:00 00 00 00 00 00 00 0D 00 44 00 61 00 76 00
69|.D.a.v.i
1BE0:00 64 00 20 00 4C 00 20 00 53 00 6D 00 69 00 74 .d. .L.

```
|.S.m.i.t  
1BF0:00 68 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .  
h.....|.....
```

The revision log in a Word document file is something that Microsoft calls "Metadata" and cannot be viewed within Word itself. I found it only by using a hex dump utility. Microsoft has an article that talks all about the problems of lingering metadata in Word documents:

<http://support.microsoft.com/support/kb/articles/Q223/7/90.asp>

It looks like the majority of virus writers who create Word macro viruses haven't read this Microsoft article. :-) I've seen many people's names in other macro virus construction kits that are distributed as Word documents.

Richard M. Smith

⚡ Re: GUIDs and Melissa (20.32)

Jiri Baum <jiri@baum.com.au>

Thu, 22 Apr 1999 02:36:50 +1000 (EST)

What's the point of a "Globally Unique ID" that isn't unique?

Presumably the algorithms that would benefit from a GUID can't use Microsoft's one, because it's far from unique; copy-and-modify is far too common a modus operandi for creating new documents, and creates collisions exactly where they're most likely to matter...

Using a pure random number would probably be better than whatever fancy schemes one may come up with, anyway. In simplicity there is strength.

Jiri Baum <jiri@baum.com.au>

✦ REVIEW: "Y2K Risk Management", Goldberg/Davis/Pegalis

Rob Slade <rslade@sprint.ca>

Wed, 21 Apr 1999 08:27:03 -0800

BKY2KRSM.RVW 990312

"Y2K Risk Management", Steven H. Goldberg/Steven C. Davis/Andrew M.

Pegalis, 1999, 0-471-33352-2, U\$39.99/C\$62.50

%A Steven H. Goldberg www.dr2000.com

%A Steven C. Davis www.davislogic.com

%A Andrew M. Pegalis www.consult2000.com

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 1999

%G 0-471-33352-2

%I John Wiley & Sons, Inc.

%O U\$39.99/C\$62.50 416-236-4433 fax: 416-236-4448

rlangloi@wiley.com

%P 312 p.

%T "Y2K Risk Management"

Bit late in the day for a Y2K book, wouldn't you say? Well, as the authors

point out, some action is better than none. And, as they also point out,

this marks your last chance to take a look at what you are doing, and make

sure you are getting the greatest benefit for your time and effort.

Chapter one is the fairly obligatory "sell or scare" piece. While similar

to others of the same ilk, it does stress the importance of interconnected and interoperating systems, as well as emphasizing the business and legal risks. On the other hand, it doesn't do a very good job of presenting the background and technical aspects, for example discussing different types of computers rather than various data structures or date usage. In the same way as many essays on building a Y2K team, chapter two looks at starting a risk management project directed at Y2K. The concepts are presented reasonably, but the details aren't terribly useful. Starting a project, and getting it up to speed as quickly as possible, is covered in chapter three. Unfortunately, the advice consists, as usual, of "get the right people, have the right plan, do the right things," with the particulars left as an exercise to the reader. Chapter four, on legal aspects, is lengthy and detailed, usually explains the concepts well, occasionally slips into legalese, sticks primarily to common law, but does sometimes lapse into the US-centric black hole. Dealing with suppliers and providers is handled much better than in most books in chapter five. One issue hinted at, but not adequately covered, is the possibility of a single point of failure removed one or more layers of suppliers from you, such as having multiple grocery suppliers--all of whose delivery fleets obtain fuel from the same source.

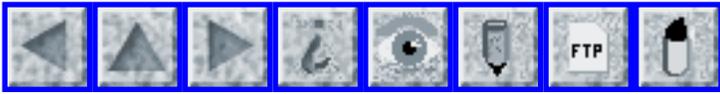
Chapter six, as did chapter three, gives the usual "do the right thing" counsel for contingency planning. Large corporate decisions and Y2K are

reviewed in chapter seven, but not really tied together. "Due diligence" was a large factor in chapter four: chapter eight looks at proving your prudence. Insurance issues are definitely not made clear by chapter nine. Chapter ten's overview of "alternative dispute resolution" (ADR: for pity's sake, *everything* has a TLA [Three Letter Acronym]!) will probably have value for many, although personally I found it rather obvious. Preparing for litigation, in chapter eleven, has a lot of very useful background, although much of it seems to assume you will be the suer instead of the suee. Post Y2K planning is brief, but touches on a number of important, and often unregarded, issues in chapter twelve.

Risk management is not really handled all that well in this book. A number of risks are identified, but the control of those hazards is left vague. On the other hand, a number of topics dealt with here get short shrift in other year 2000 guides. Overall, while I couldn't recommend it as the only reference for those just starting out, I would say that, for those seriously into Y2K planning, the book should handily repay the price and time spent on it.

copyright Robert M. Slade, 1999 BKY2KRSM.RVW 990312
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

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



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 34

Weds 28 April 1999

Contents

- [Virus infects computers worldwide](#)
[Edupage](#)
- [A genuine sighting of a virus -- for once](#)
[Nick Brown](#)
- [Sex aid give holiday flight a shaky start](#)
[Frank Markus](#)
- [A Supreme Indecency](#)
[Monty Solomon](#)
- [Bar says e-mail OK for transmissions](#)
[Monty Solomon](#)
- [You'd think they'd know better...](#)
[T Bruce Tober](#)
- [A man charged with counterfeiting bank ATM cards](#)
[Chiaki Ishikawa](#)
- [What's DejaNews up to?](#)
[Richard M. Smith](#)
- [Dodgy automatic address book resolution](#)
[Samuel Liddicott](#)
- [Re: GUIDs and Melissa](#)
[Russ Cooper](#)

- [REVIEW: "Great Misadventures", Peggy Saari](#)
[Rob Slade](#)
 - [Open Source Software at 1999 USENIX Annual Conference](#)
[Jennifer Radtke](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Virus infects computers worldwide

Edupage Editors <edupage@franklin.oit.unc.edu>

Wed, 28 Apr 1999 12:41:33 -0600

The Chernobyl virus yesterday attacked more than 600,000 home, office, and government computers around the world, causing an estimated hundreds of millions of dollars in damage. The virus, which struck on the 13th anniversary of the Chernobyl nuclear explosion and is named for the disaster, is believed to have its roots in Taiwan. Windows 95 and Windows 98 files are attacked by the virus, which tries to erase the hard drive and prevent the computer from being booted. However, no large-scale system failures have been reported. In the United States, reports of 2,328 infected computers at 228 locations were made to the Computer Emergency Response Team at Carnegie Mellon University. The most severely impacted country appears to have been South Korea, where as many as 300,000 computers were affected by the virus. The virus may have damaged as many as 15 percent of all computers in South Korea, and could cost the country \$250 million, according to a South Korean news agency's quotes of industry experts. In Turkey, computers were affected at an airport, a

military

academy, the state-run radio and television station, and several banks.

Electronics engineer Mustafa Ucklar says Turkey was caught unprepared and

the country had not taken notice of warning signs. (*The Washington Post* 28

Apr 1999; Edupage, 28 Apr 1999)

✦ A genuine sighting of a virus -- for once

BROWN Nick <Nick.BROWN@coe.int>

Tue, 27 Apr 1999 09:20:40 +0200

I dropped into my friendly neighbourhood computer dealer last night to find not one but two guys standing there with their PCs. Both with the same symptom - CIH/Chernobyl had trashed their BIOS. For once, a virus really struck ! That's two in one day in Molsheim, France (pop 8,000).

One of the PCs was from the shop itself, and the owner was obviously a hacker. He took it in reasonable spirits, although round here he'll probably be \$75 down for a new BIOS chip. The other was from a local hypermarket, seven months old. I suggested to the owner that he take it back to the shop under warranty. This kind of store can't do proper after-sales for software problems, of course, but they might be persuadable that a completely black screen at startup could be a broken motherboard.

In fact, it would be interesting to see what various countries' consumer

laws make of "my BIOS was trashed by a malicious program, and my PC no longer boots". PC stores (and corporate support desks) already have quite enough people expecting them to fix problems caused by screwing around with OS files, but how responsible can someone be for the care of their BIOS chip?

The RISK ? Well, apart from the obvious virus-related ones, there's the problem of getting repairs under warranty in those grey areas between "the system broke" and "you broke the system".

Nick Brown, Strasbourg, France

✶ Sex aid give holiday flight a shaky start

"Frank Markus" <fmarkus@pipeline.com>

Sun, 25 Apr 1999 06:26:07 -0400

A pilot made an emergency landing when a suspect device was detected on a jet packed with British holiday makers -- but the threat turned out to be a sex-aid vibrator.

The A-300 Monarch Airbus was two hours into a flight from Goa when the crew became suspicious about a piece of hand luggage. The pilot, Captain Dave Johnson, radioed a bomb alert and was ordered to divert to Bombay.

The plane, carrying British-based passengers and crew, was taken to an isolated handling bay where 369 people were evacuated. Bomb disposal experts boarded the plane and examined the suspect

baggage and
identified the device as a battery-powered sex vibrator.
A Monarch Air spokeswoman applauded Capt Johnson's actions. "We
are looking
into the incident to find out how it got on board," she said.
The passengers
later continued to Gatwick.

I initially found this story in rec.travel.airlines on Usenet.
I followed
the links in that message to the actual article (above, Tuesday
April 20,
11:01 AM). The next message posted was from an airline ramp
agent:

"Actually, this kind of thing happens way too often.
I used to work for a major airline as a ramp agent, and I'd
put the
number at 2-3 times per year, per airline.
What happens is a bag (usually checked though) gets jostled,
and
vibrator switches on, bag starts buzzing or humming, employees
alert
security, and then the real fun begins.

"Our SOP used to be offload pax, have them claim baggage on
ramp, then
swoop in on suspicious bag. have pax reveal source of buzz,
worst
embarrassment of life ensues, in front of planeload of angry,
delayed
strangers. It was ALWAYS the best part about working the
ramp. And this
should serve as a cautionary note, pack the batteries separate
if
traveling with a vibrator."

I love this story. It has everything that is required for an
urban legend

but it is true. The original story is still available at:

[http://www.yahoo.co.uk/headlines/19990420/london/
newsstory133839.html](http://www.yahoo.co.uk/headlines/19990420/london/newsstory133839.html)

[I thought maybe the "vibrator" was related to the vi editor, since "vi" is s*x in Roman numerals. PGN]

✶ A Supreme Indecency

Monty Solomon <monty@roscom.com>

Wed, 28 Apr 1999 10:57:32 -0400

Congress tried to make it a felony to say anything "indecent" online

"with intent to annoy" another person. The Supreme Court has just decided the appeal in the case testing the law.

It had to be the shortest Supreme Court decision on the merits of a

First Amendment issue ever: "The judgment is affirmed."

ApolloMedia

Corp. v. Reno, No. 98-933 (April 19, 1999).

<http://www.lawnewsnetwork.com/opencourt/stories/A939-1999Apr27.html>

✶ Bar says e-mail OK for transmissions

Monty Solomon <monty@roscom.com>

Wed, 28 Apr 1999 10:50:33 -0400

The American Bar Association has given its seal of approval to the use

of e-mail to transmit client documents.

Under most circumstances, a lawyer does not violate a client's confidentiality by transmitting documents via unencrypted electronic mail,

the ABA Standing Committee on Ethics and Professional Responsibility

concluded in an ethics opinion announced last week.

<http://www.lawnewsnet.com/stories/A953-1999Apr27.html>

✶ You'd think they'd know better...

T Bruce Tober <octobersdad@reporters.net>

Sun, 25 Apr 1999 13:13:34 +0100

...or maybe not. I mean, it is Microcrap we're talking about here, viz this article from Woody's (Woody's Office Watch), and if there's anyone more pro-Microsoft it's only Bill G himself, : (Read the complete story <http://www.wopr.com/>)

TRUST NO ONE [...]

Microsoft has in the past released virus infected documents on their web

site and by other means. WOW has had to publish warnings several times.

Sadly it's happened again. Anyone visiting http://www.microsoft.com/uk/business_technology/dns/ecommerce/financial/case.htm

to find out more about MS Exchange and E-commerce got more than they

bargained for when they downloaded any of the case study documents. All

were infected with W97M/Marker.C virus! Apparently no-one at Microsoft

checked the documents before making them publicly available [...]

Bruce Tober, <octobersdad@reporters.net>, <<http://www.crecon.demon.co.uk>>

Birmingham, UK, EU +44-121-242-3832 soon at <<http://www.star-dot-star.co.uk>>

✦ A man charged with counterfeiting bank ATM cards

Chiaki Ishikawa <Chiaki.Ishikawa@personal-media.co.jp>

Thu, 29 Apr 1999 04:43:00 +0900 (JST)

Lately about a dozen people whose account reside in two Japanese banks found their money withdrawn by unknown third party. Police began investigating and found, from the video tape recording of the ATM machines where withdrawals took place, a man seemed to have used fake bank ATM cards and withdrew the money from ATM machines in Tokyo area.

Last week, the police arrested a man and charged him for the theft.

But how did this man find about the existence of the bank account and that the man found the password or PIN? It turns out that the man worked for a software company that subcontracted the reservation system maintenance for a city-operated resort facility from an NTT group company. All the people whose money was stolen made a reservation to the city facility at least once.

The city resort facility takes reservation from its citizens with advance partial payment. The hitch is that when the applicant cancels the reservation, the advance payment is returned to the applicant's bank account. For this purpose, the city office records the bank account information as well as other personal information such as telephone number,

address, etc. in the database. All these reservation and cancellation work seems to be done via computer terminal.

The culprit who works at the company that manages the host computer for the reservation system obviously had access to the database of the reservation including the bank account (no encryption that keeps the maintenance operator to look inside?). So he could concoct a new ATM card by recording the information onto a magnetic-strip card using a magnetic card writer.

Now the second big question is how he figured out the PIN. (The card itself no longer carries PIN on itself.) Well, it seemed easy to him. Since he had access to the personal information such as telephone number, address, etc., he seemed to make educated guesses and obviously he succeeded. Sigh...

In the same article, some banks were quoted as thinking of making it possible for customers to change the PIN regularly. (I am not sure if this works well. If someone picks up bad password, will the person pick up good password next time? There may be human risks here, but am not sure.) For that matter, PIN for bank ATM cards here in Japan are only 4 digits! Shoulder-surfing certainly is possible.

Also, I just learned today that the culprit stole other people's bank cards in trains and so forth so that he could overlay the stolen bank account information on these cards to try his guessed PINS. Any physical checking done by the card reader itself seems to have been

thwarted by the culprit's using otherwise genuine ATM cards. However, I don't know if any such checks are done by the card readers and cards used today in Japan. Maybe the culprit was very cautious. Police reportedly found fake credit card as well at the culprit's home, so in that case, nice-looking holograph, etc. was necessary for counterfeiting.

A few risk lessons from this incident:

Private database with sensitive information should be encrypted so that only the appropriate user can access its contents. The night-shift operator who do backup can carry a duplicate copy, etc.. Also, proper auditing of access to the database could deter such criminals. In this case, the city office could use a PC for terminal and use plain text information on that terminal alone and could store the encrypted information at the host computer managed by the company where the culprit works. (Sure, the search against the stored data record might be an issue here. But by storing the name in plain text and the rest in encrypted form, it should pose no big problem IMHO.)

ATM cards should be hard to fake in the first place. The bank officials were quoted in an Asahi shimbun article as saying that making counterfeiting like this impossible is very difficult technically.

I wonder if adding some information on the card, such as the md5 checksum of the concatenation of the closely kept secret master bank seed string + the ordinary information on the card such as the branch number, account number,

holder's name, etc. could make the counterfeiting more difficult. Unless the counterfeiter knows the secret seed string it becomes impossible to fake the ATM. I guess such scheme would make the counterfeiting very difficult. But the bank people may not want to upgrade all the ATMs across the whole of Japan at once, or it may be that the ATM card used today may not hold all the md5 digits or even reasonable length of it capacity-wise. But probably they'll be forced to upgrade the security anyway by the social pressure in not too distant future. I was very surprised about this counterfeiting being so easy myself.

Also, as has been said million times, don't use the obviously easy to guess PINs based on your telephone number, birth date, etc.. I am not sure if the database in question contains the birth date for the purpose of the reservation, but since the success rate seemed to have been high, it could. But if so, I will add another lesson here.

Don't collect unnecessary personal information. It will leak out or be abused in some way or the other. (Chiaki's law a la Murphy's law.)

Will computer IC card solve these counterfeiting problems in the future?

Chiaki Ishikawa <ishikawa@personal-media.co.jp.NoSpam>
Personal Media Corp., Shinagawa, Tokyo, Japan 142-0051

⚡ What's DejaNews up to?

"Richard M. Smith" <rms@pharlap.com>

Sun, 25 Apr 1999 15:21:14 -0500

One of my favorite Web sites is DejaNews, the search engine for Usenet newsgroup messages. Yesterday I discovered a new "feature" of DejaNews which I don't understand.

It seems that when a newsgroup message containing URL's is displayed, the DejaNews server is silent changing the links to be routed through the DejaNews servers. This new feature allows DejaNews to track when a person clicks on a Web site link in a newsgroup message. You still get to the Web site, you just go through the DejaNews servers first. My understanding is that the new feature was added a couple of months ago.

Here is a quick example of what DejaNews is up to:

Original link: <http://www.yahoo.com>

Tracking link: <http://x12.dejanews.com/jump/http://www.yahoo.com>

Apparently the DejaNews servers simply redirect your browser to the real URL after recording where you clicked. In the newsgroup message itself, the original link is shown, not the tracking link.

An easy way to defeat this tracking mechanism is to manually copy the link in the message text to the location or address window of your browser.

I ran a simple experiment and found that a Web site will still get the referring URL which is the URL of the newsgroup message. So one thing that DejaNews is not trying to do is block Web sites from knowing

where a click
came from.

Pretty obviously, DejaNews knows a lot about me already by my
searching
habits. Why do they now also need to know what Web sites I'm
visiting?

What is being done with this information?

Pretty odd if you ask me. What I can't figure out is what
DejaNews is up to
here. Does anyone have any ideas?

Richard M. Smith <smiths@tiac.net>

[Added note: It gets more interesting. DejaNews is also
tracking

e-mail addresses. When one clicks on an e-mail address in a
newsgroup

message, it first goes thru the DejaNews server before being
redirect as a

mailto: URL. DejaNews ends up know who and when someone is
sending e-mail

to. This is just plain weird.]

Here is more info from comp.security.misc:

donoli wrote:

> Exactly. Since they are chaining the URL, they get credit for
bringing

> users to the second site.

Yep, Web sites with high click-thru rates get called first by
their friendly
DejaNews ad rep!

Maybe the next step here for DejaNews is to somehow figure out
how to charge

Web sites for click thru's. Toll booths on the Internet? For
example, maybe

DejaNews only highlights links for Web sites that have DejaNews
accounts. Each click-thru then costs a dime.

Why DejaNews went through all of the trouble to also track e-mail makes no sense at all. It's just plain rude. I've asked their privacy people and PR people what's going on. Hopefully they'll get back to me today.

BTW, According to Junkbusters.com, the hotbot search engine also does the same trick for Web sites. They are tracking click-thru's in search results. None of the other major search engines (AltaVista, Yahoo, Lycos, and InfoSeek) appear to be doing this.

Richard

✶ Dodgy automatic address book resolution

"Samuel Liddicott" <sam@campbellsci.co.uk>

Mon, 26 Apr 1999 09:42:19 +0100

I work at Campbell Scientific.

It's not surprising that the managing directors has a last name "Campbell".

(Lets pretend his first name is Bill)

I have IE5 and Outlook 98. In my address book is a local employee who shares the same first name as the overseas director. (Let's pretend it is Bill Prescott)

In an e-mail message I typed:

Bill Campbell

as the recipient, which my address book foolishly resolved to "Bill Prescott

<bill@campbellsci.co.uk>

Doh! Just because there is a Bill in my address book with campbell in his e-mail address!

The risks? Expecting technology to abide by my definition of sensible. I thought I was typing a full name, the computer in its attempt to "do the right thing" was a little too eager. I was expecting the address book to fail to resolve, and that it would be picked up by the LDAP server.

The even worse risks? That "Bill Campbell" would work until "Bill Prescott", a distinctly different name appears in the address book.

Finally, in an effort to make software "do the right thing", it is worth evaluating when this might turn out to be a "very wrong" thing.

Sam Liddicott <sam@campbellsci.co.uk>

✉ Re: GUIDs and Melissa (Baum, [Risks 20.33](#))

Russ <Russ.Cooper@rc.on.ca>

Mon, 26 Apr 1999 23:08:06 -0400

>What's the point of a "Globally Unique ID" that isn't unique?

With all due respect, this isn't "Microsoft's one", its the OSF's definition of how to create GUIDs. Copy-and-modify puts your GUID on the modified document (over-writing the previous GUID), whereas cut-and-paste puts other

content in a document with your GUID.

The GUID wasn't intended to uniquely identify the document, only the OS/Application installation it was created/last modified on.

For those that forget, NT 3.1 (from which all this GUID stuff stemmed for MS) was largely based on OSF/DCE. Arguments aside, they did implement the GUID creation process according to DCE spec.

Russ - NTBugtraq moderator

REVIEW: "Great Misadventures", Peggy Saari

"Rob Slade, doting grandpa of Ryan and Trevor" <rslade@sprint.ca>
Tue, 27 Apr 1999 08:42:19 -0800

BKGRMSA.RVW 990318

"Great Misadventures", Peggy Saari, 1999, 0-7876-2798-4, U\$99.00
%A Peggy Saari
%C 27500 Drake Road, Farmington Hills, MI 48331-3535
%D 1999
%G 0-7876-2798-4
%G (0-7876-2799-2 0-7876-2800-X 0-7876-2801-8 0-7876-2802-6)
%I The Gale Group/Gale Research Inc.
%O U\$99.00 248-699-4253 fax: 800-414-5043
%P ~800 p.
%T "Great Misadventures: Bad Ideas That Led to Big Disasters"

Let us start with some cliches. Life is a hard teacher: she gives the test first, and the lesson afterwards. Good judgement comes from experience: experience comes from bad judgement. Those who do not learn from history (or History 205) are doomed to repeat it. We learn far more from failure

than we do from success. And, finally, learn from the mistakes of others:

you will never live long enough to make them all yourself.

If there was ever a book concept made for the RISKS-FORUM Digest library

(aside from PGN's own) it is this: great boneheaded ideas from the past. In

this junior edition, four volumes divide that topic into exploration,

science and technology, military, and society.

Unfortunately, while the essays provide decent canned histories of the

events, they make lousy lessons. All of the material is presented at the

same level of very rough detail, rather than sketching in a background and

then concentrating on a specific mistake. A number of decisions in any

chapter may be identified as errors, but there is little commentary on why

the action was wrong and contributed to the disaster in question. Why did

this endeavour, intended to promote safety, ultimately spell catastrophe?

If this person or institution was motivated by greed or ambition, at what

point did the driving force behind development become a destructive power?

While there is a lack of analysis overall, a particular failing is the lack

of examination of options that might have changed the outcome for the

better.

In the Reader's Guide starting each volume, the point is made that a

calamity had some positive result, usually in terms of a reform or

improvement. Relatively few of the stories, however, tell of any such

correction. In both the Apollo 13 and Bre-X articles, in fact,

the text has
to admit that we do not know for sure what the causes of the
problems were,
and therefore no lesson can be drawn from them at all.

Of greatest interest to the largest number of readers of this
series will be
the article on the Year 2000 problem, otherwise known as the
millennium bug
or Y2K. Perhaps the kindest thing that can be said about this
essay is that
it will become academic in less than a year. The situation is
blamed on an
"error" (with no mention of the widely used standard), although
the next
paragraph states that it should not be called a "bug." Although
Peter de
Jager has worked tirelessly to bring the issue to the attention
of the
public, it is not true that nobody knew about it before his 1993
article. I
have never seen any microwave oven that cared what the date was,
and it is
rather beyond the bounds of probability that an aircraft would
shut down in
flight because it felt miffed at being too long without a
checkup. An
entire section of the article confuses the predicament with the
unrelated
issue of maintaining archival records as generations of storage
hardware and
media pass by. The entire disaster is ultimately laid to the
blame of
"negligent" computer developers.

There are a number of sidebars, generally giving a biography of
involved
characters, and illustrations. The biographies sometimes seem
at odds with
either the essays of which they form a part, or oddly placed in
proximity to
more detailed accounts, and the figures, where placed in a
piece, provide

little explanatory support. The military section, for example, has numerous battle maps where the order of a campaign is extremely difficult to follow. (Yes, I know: war is messy.) Some of the diagrams, as originally produced, were probably supposed to be in colour, since the keys cannot, in the black and white version, distinguish between items of opposed significance. Much material is duplicated between pieces, but even that can be confusing at times. Many terms are explained in article after article, and the explanations are not always consistent. A musket will be defined as a "shoulder gun" in one essay, a "rifle" in another, and a "gun like a rifle" in a third. Not a great difference, but confusing. (The index does not assist in clarifying matters: there are lots of entries for people, but almost none for things.)

The cachet of disaster might make this an inviting set for promoting study of history in a rather "dates of the kings of England" manner. The events are isolated, the details are scanty, and the analysis almost doesn't exist. I doubt that students would learn much of either history or judgement from these books.

I should add, in view of the topical relation to the Risks Digest, that PGN's book is not only cheaper and *way* more accurate, but it's also more fun to read.

"Computer-Related Risks", Neumann, 1995, 0-201-55805-X, U\$24.75

And it's possibly also time to mention Lauren Wiener's book

again as well:

"Digital Woes", Wiener, 1993, 0-201-62609-8, U\$22.95/C\$29.95

copyright Robert M. Slade, 1999 BKGRTMSA.RVW 990318
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

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

✈ Open Source Software at 1999 USENIX Annual Conference

Jennifer Radtke <jennifer@usenix.ORG>

Tue, 27 Apr 1999 16:11:59 GMT

[Item abridged for RISKS. PGN-ed]

*** Registration Savings until 3 May 1999 ***

Top developers, systems administrators, and other UNIX gurus get the why as well as the how-to at the reknown USENIX Annual Conference. The USENIX Conference takes place June 6-11, 1999, in Monterey, California. Programs for the tutorial and technical sessions, including the FREENIX track, and associated events are online. Please go to <http://www.usenix.org/events/usenix99>

The FREENIX track is devoted to high-level technical discussion of open-source software. USENIX has also provided a grant to the OpenBSD development project to support a new release. It will be distributed for free at the conference. USENIX is helping to ensure that the development process for open source software will continue to be

characterized by
intense yet healthy competition.

The refereed papers are on topics of especially high interest:
management
of resource systems, file systems, virtual memory systems,
storage systems,
security, web server performance and O/S performance. The
Invited talks
concentrate on the extremely practical; topics include: UNIX/
Open System &
Y2K, IP Multicast, e-mail Bombs, IPv6, IP Telephony.

John Ousterhout, creator of Tcl/Tk and leading figure in the
open source
world will deliver the conference keynote. His attention is on a
fundamental shift in software development to integration
applications --
created by coordinating and extending existing applications,
protocols,
frameworks, and devices.

24 tutorials are being offered over three days, with Eric
Allman, Tom
Christiansen, Peter Galvin, Evi Nemeth, and Marcus Ranum among
the
instructors. Courses range over systems administration,
security, Linux,
high availability, kernel internals, Perl, performance tuning,
network
programming and configuration, and more.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 35

Friday 30 April 1999

Contents

- [On-line banking customers off-line for the week](#)
[PGN](#)
- [Court labels unwanted e-mails "trespassing"](#)
[NewsScan](#)
- [13-year-old makes \\$3M in bids on eBay](#)
[Doneel Edelson](#)
- [File-conversion errors between Word and WordPerfect](#)
[Gordon Foreman](#)
- [Re: The Bloatware Debate](#)
[RA Downes](#)
- [Flash BIOS risks](#)
[Jonathan Levine](#)
- [Re: What's DejaNews up to?](#)
[Col. G.L. Sicherman](#)
- [RISKS of the net's success...](#)
[Matt Curtin](#)
- [IWC Watch Company site publishing visitors e-mail addresses](#)
[Derek Ziglar](#)
- [Risks of misaddressed mail](#)
[Joe Thompson](#)

- [REVIEW: "The Y2K Survival Guide", Bruce F. Webster](#)
[Rob Slade](#)
 - [Advanced Workshop: USENIX Smartcard Technology, May 10-11, Chicago](#)
[Jennifer Radtke](#)
 - [CFP, 1st European Anti-Malware Conference](#)
[Jaroslav Blaha](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ On-line banking customers off-line for the week

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

Fri, 30 Apr 99 9:45:34 PDT

A glitch in the networking software in the Genesis system at CheckFree in Atlanta has caused repeated crashes affecting the operations of at least 21 banks nationwide since Monday 26 Apr 1999. Wells Fargo said as many as 150,000 of its customers using Quicken or Microsoft Money to pay bills were blocked, although its other 710,000 on-line customers paying bills directly have not been impeded. (We previously reported on-line brokerage systems saturating because of increases in demand.) [Source: Sam Zuckerman, *San Francisco Chronicle*, 30 Apr 1999, B1; PGN-ed]

⚡ Court labels unwanted e-mails "trespassing"

"NewsScan" <newsscan@newsscan.com>

Thu, 29 Apr 1999 08:17:45 -0700

A California court has ruled that mass e-mails sent to Intel workers by a

disgruntled former employee were an illegal form of trespass, setting a new legal boundary between private computer networks and the public Internet.

The case had centered on a barrage of unsolicited e-mail messages sent by Ken Hamidi, who'd been fired in 1995, criticizing Intel's workers' compensation policies and other issues. Intel had sued Hamidi, charging misuse of the company's computer networking resources, and Judge John R.

Lewis agreed, comparing borders between computer networks to property boundaries: "The mere connection of Intel's e-mail system with the Internet does not covert it into a public forum." Meanwhile, some legal scholars

questioned the judge's analogy: "In the real world, trespass involves physical presence," says Jonathan Zittrain, a law lecturer at Harvard. "But in this case, it's his speech they're restricting." However, the judge

noted that Intel has never published its employees' e-mail addresses, strengthening its argument that its computer system is private company property rather than a public gathering place. (*Los Angeles Times*,

29 Apr 1999, <http://www.latimes.com/home/business/t000038417.html>)

✶ 13-year-old makes \$3M in bids on eBay

"Edelson, Doneel" <doneeledelson@aciins.com>
Fri, 30 Apr 1999 13:05:31 -0400

Using his parents' eBay account, an eighth-grader named Andrew

Tyler bid more than \$3M on items such as \$1.2M for a medical office in Jacksonville, \$.5M for a Van Gogh painting, \$35,000 for a Viking ship replica, \$120,000 for the first Superman comic. He also bid on a 1955 Ford convertible, a 1971 Corvette, and a bed that once belonged to Canada's first prime minister -- for which he offered \$900,000 on the previous bid of \$12,000. In addition to high-bidding the bed, he had four other successful bids, and clearly upped the ante on others. It was apparently just like another computer game to him. Yes, you might ask, eBay has a policy against under-aged bidders, but until now it has been on the honor system. [Source: USA Today - Tech Report, 29 Apr 1999; PGN-ed]

✶ File-conversion errors between Word and WordPerfect

Gordon Foreman <u098348@lanl.gov>
Thu, 29 Apr 1999 13:50:37 -0600

DoE just posted this to all contractors and offices. It is certainly not classified, so I thought it might be interesting to your readers.

<begin quote>
FYI - this information was received from the DOE Lessons Learned List Server on 4/27. Please share it with the appropriate people in CIC. I also forwarded it to cic-news@lanl.gov and the NewsBulletin.

- - - - -

Project Hanford Lessons Learned
Title: Characters Convert Inaccurately Between Word Processors

Date: April 20, 1999

Identifier: 1999-RL-HNF-0018

Lessons Learned Statement:

Documents converted from WordPerfect into Microsoft Word may contain errors in character mapping that could cause serious problems and potentially unsafe conditions, especially with operating procedures and other safety-related documents.

Discussion of Activities:

Documents converted between word processing software packages may contain incorrect characters caused by inaccurate mapping between character sets. Some fractions may not convert accurately. This could create safety issues if operating procedures were released with erroneous information. For example, the fraction 1/4 in WordPerfect® converts to a value of three (3) in Word. An operating procedure that states, "Open valve A-45, Holding Tank Fill Valve, 1/4 turn." would read "Open valve A-45, Holding Tank Fill Valve, 3 turn." after conversion.

Analysis:

There are basically two problems. One deals with font substitution and the other deals with the way Word converts symbols into characters. The problem related to font substitution is an issue with any Windows application. As technology improves, so have the character definition standards. Word uses a relatively new character definition standard called Unicode that assigns a unique 16-bit number to each symbol or character. WordPerfect 5.1 uses a character set called OEM (original equipment manufacturer).

Older Windows

applications use a standard character set called ANSI (American National Standards Institute). The 3 standards are not the same for all characters, especially for symbols and characters beyond the normal letters and characters on the keyboard. A word processor opening a file with a character set that it does not use may not map each character to the correct symbol in its own set. Users opening a document on a system that does not have the same font set as that used in the original document may see unexpected results on their screen such as boxes or other strange characters, due to font substitution.

The other problem arises from the way Word treats some symbols as codes and others as characters. The character symbols are more susceptible to changing when the document base font is changed. The character may change to an empty box, or a character from a different font set. To prevent this, the character symbol should be changed to a code symbol.

Any document with any character set created using any version of WordPerfect may be susceptible to this problem. Other word processors may also cause these errors.
<end quote>

Gordon Foreman, Los Alamos National Laboratory

[Note: I have removed all of the repeated \256 characters after "Word" and "WordPerfect" for the benefit of those noncompliant mailers that block the entire issue if there is a single extended-ASCII character in RISKS. The astute reader must mentally reinsert them, so that RISKS is

not in
violation of the trademark conventions. PGN]

✶ Re: The Bloatware Debate

<main@radsoft.net>

Fri, 30 Apr 1999 16:22:48 +0000

One of the chief hallmarks of early UNIX was how simple, compact programs worked well together. Brian W. Kernighan's definition of a good program was a program so good and so consistent that it could be used for an entirely different purpose and be expected to work well. UNIX, they said, was a way of thinking more than an operating system. And, with Brian's Software Tools series, it was surely so.

Microsoft Windows is also a way of thinking - or not thinking, to be more exact. In almost every possible sense it is the anathema of the programming community, if that community still abides by and adheres to the solid thinking delineated by Brian so many years ago.

MS Windows programming is considered too difficult to attempt head on.

Where we come from most major corporations, financial institutions and the like promised a smooth transition from UNIX or DOS to Windows 3.1x within a matter of weeks. Management talking of course. When they found this would not work they decided to invest heavily in 16-bit Visual Basic applications. Operative word "heavily". These bloatware masters sunk almost any machine made. Clearly this was not the answer either.

People looked to Kahn. Borland, with its Turbo C, saw the opening and released Borland C, and shortly thereafter Scott Randell who a year earlier had toured with MSC 7.0 (which admittedly never worked) was out rocking again, this time with Visual C++. The environment was unbelievable; the executables were extremely bloated; but still and all it was Microsoft talking, and still and all they were smaller than the corresponding Borland images. COBOL programmers everywhere were suddenly encouraged to learn C++, develop code browsing skills, learn about preprocessors, assembly language, CodeView and subsequent debuggers, and the world entered into a tailspin.

What originally started as a rather feeble but lucky attempt to get on the OO bandwagon, the MFC soon became something you'd like to see Steve McQueen kill. Patches and work-arounds and bugs and more bugs, and bloat and more bloat. The current splash screen module is a case in point: Microsoft includes a 16-color bitmap which weighs in at nearly 200KB for you. This bitmap can be compressed with RLE encoding to less than half that size. The idea of banging a 100KB splash bitmap in an application is still, however, sickening. Yet Microsoft gladly gives you the bitmap at 200KB, happy if you don't understand what you are doing by using it. Your application will be more sluggish than their own bloatware, and people will be less inclined to complain about what they themselves do.

Microsoft's RegClean, a popular product for fixing corruptions

in the MS
Windows Registry is another case in point. When this application
was
originally introduced I downloaded it and wondered about its
size. It
weighed in then at nearly a megabyte. Similar applications out
there were
20KB and hardly more. What was inside this monster? I opened it
and looked
inside.

Remember all those stories about how surgeons in the old days
just threw
their rubber gloves inside the patient's stomach before sewing
them back up
again? Well here you had it. There were humungoid bitmaps never
used. There
were dozens of icons never referenced. There were tens of
kilobytes of
entries in the string table that had no meaning for the
application
whatsoever.

I honed the app down and came to the conclusion that the actual
size of
RegClean should be about 45KB. That as compared to its
distribution size of
nearly one megabyte. Clearly bloat is not only a question of
adding features
almost no one wants. Bloat is a condition of the mind,
permeating software
houses everywhere.

Clearly again the distribution of RegClean was highly
irresponsible. But
remember, MS Windows is not just an operating system - it is a
way of
thinking, or not thinking as you may have it. And it has
permeated the
entire industry today. Our hats off to Microsoft.

In conclusion: there are few application domains even today that
require

executables of over 100KB, and most ordinary tasks can be adequately managed

by executables in the 20KB range. This is simply a fact.

There are no excuses. Either we think or we don't. There is no in between.

RA Downes Radsoft Laboratories <<http://www.radsoft.net>>

✶ Flash BIOS risks (Re: Genuine sighting, Brown, [RISKS-20.34](#))

Victor the Cleaner <jonathan@canuck.com>

Thu, 29 Apr 1999 01:13:27 -0600 (MDT)

My take on this is a little different. I'm a embedded control designer known by local component suppliers to have a lot of device (chip) programming equipment, so people are regularly directed to me for memory and microcontroller burning. Hey, it's beer (okay - single malt) money.

This week I had somewhat more than the usual number of calls regarding PC Flash BIOS chips needing reprogramming. Whether this was the result of one of these reportedly BIOS-hungry viri or a coincidentally high number of failures of user-initiated BIOS upgrades I haven't determined.

My attention is drawn to the latter. As a designer, I find it hard to grasp the thinking behind crippleware-in-waiting - systems such as these that rely on high-level functionality to perform low-level [firmware] changes without a net. If, for any reason, the operation does not complete properly, the machine is hosed hard.

The RISK is the lack of a Plan B - any bootstrap method of recovery from such a failed upgrade. As is, the victim has the choice of either tracking down what for the average consumer must be a truly obscure and arcane service (someone who can copy the BIOS-vendor's binary from a floppy to the chip) or just calling the whole damn thing DOA, as suggested by Nick Brown.

Jonathan Levine, Canada Connect Corp., Calgary

⚡ Re: What's DejaNews up to? (Smith, [RISKS-20.34](#))

Col. G. L. Sichertman <colonel@monmouth.com>

30 Apr 1999 13:52:38 -0400

I don't know what commercial advantages DejaNews may gain by tracking clicks, but this can be helpful to users of any search engine. For example, consider a search on

bambi book children

The first two entries on the list are:

1. Book exotic dancer Bambi for your next stag party! Not suitable for children. ...
2. Bambi, by Felix Salten, is a wonderful book for children. Here's how to order: ...

Most people will select item 2. Knowing this, the search engine will

start presenting item 2 at the head of the list. It's an automatic way to make search engines more helpful--at the risk of making it harder to find things that most people don't want.

Col. G. L. Sicherman web: <<http://www.monmouth.com/~colonel/>>
work: sicherman@lucent.com home: colonel@mail.monmouth.com

[... and they are easily Bambioozled. PGN]

⚡ RISKS of the net's success... (Re: DejaNews, Smith, RISKS 20.34)

Matt Curtin <cmcurtin@interhack.net>
29 Apr 1999 14:30:37 -0400

As noted, this business of tracking links is not new. DejaNews and HotBot aren't the only ones doing this, either.

In other strange-but-true news, after releasing a report that was generally critical of Netscape's implementation of the "Smart Browsing" feature, we discovered that that very feature was claiming our report is "related" to the Unabomber Manifesto. A good summary of this was covered in Lauren Weinstein's PRIVACY Forum Digest 08.06[1]. It was also reported that AltaVista is preparing to give preferential treatment in search results to those who pay for their listings. [In Lauren's PRIVACY item, he noted that AltaVista says that those listings will be marked as having been paid for.
PGN]

Lauren made a really interesting point in the PRIVACY Forum

Digest that really seems to cut through all of the noise around these annoyances and problems, getting to the larger problem, that is the risks associated with the Internet's success. He wrote:

It's of enough concern when we learn that major search engines (e.g. AltaVista) are about to start selling search result placements. It's of equal concern if users need to be worried that other search results, returned by other search engines, might

potentially be skewed by unobvious forces not related to an unbiased analysis of the sites in question, even if monetary considerations are not the factor involved.

If search engines begin to lose the trust of their users, one of

the net's most powerful category of tools may be reduced to nothing more than automated pitchmen using every means possible,

no matter how biased, to try pull the yokels into the tent. In that case, it will not only be a serious loss for us all, but will

also create the potential for a sort of "information pollution" on

a scale we've never seen before.

Is it possible that the success of the net will lead to its own demise

from the perspective of a useful resource that serves its end users?

[1] <http://www.vortex.com/privacy/priv.08.06>

Matt Curtin cmcurtin@interhack.net <http://www.interhack.net/people/cmcurtin/>

⚡ IWC Watch Company site publishing visitors e-mail addresses

"Derek Ziglar" <anon@dziglar.com>

Thu, 29 Apr 1999 13:23:14 -0400

IWC, a Swiss manufacturer of high-end wristwatches, has opened up a severe privacy invasion on their web site at <http://www.iwc.com>. In an all too common RISK, I'm sure the site designers or company executives thought it would be cute to display the names of the 10 most recent visitors to their site on their main page.

The privacy issue is that they ask for your name and e-mail as part of a sign-in on initial entry to the site -- then immediately display on their main page your name along with 9 other recent visitors to their site as a mailto links with each person's e-mail address!

As RISK readers are well aware, this would be an easy point for someone unscrupulous to harvest e-mail addresses. Similarly, a user could enter obscenities or other information that IWC would likely not desire to display on their web site.

There is no way for a first time visitor to know that their information will be publicly displayed until it is too late. There are no provisions to opt out or have the information removed (except for it to age off the list after 10 more people sign in to their site). The information is stored in a cookie under your browser and redisplayed if you return to the site via bookmark -- unless you enter through the welcome form and blank out the fields before continuing.

IWC International Watch Co. Ltd., Baumgartenstrasse 15, CH-8201 Schaffhausen, Tel: +41 52 635 65 65, Fax: +41 52 635 65 05, info@iwc.ch

✶ Risks of misaddressed mail

Joe Thompson <spam+@orion-com.com>

Thu, 29 Apr 1999 15:50:30 -0400

Recently I got a message that looked like a lot of the spam I get; it was a business-style e-mail with a Word attachment, talking about a "business proposal". It wasn't addressed to me; I figured I had gotten on Yet Another Spam List and left it in the "spam" folder it had been filtered to.

Today I got what appeared to be a follow-up mail. Same originating address. This time I looked at the full headers of both messages. It didn't look like any games had been played with open relays and I started wondering if this could be legitimate mail that had gotten misdirected.

A moment's digression: I have a "blind forward" on the domain I own, so all mail addressed to my domain goes into my main mailbox unless specifically directed elsewhere. This means I can make up aliases "on the fly" for things like web form registration, which allows me to receive legitimate mail but also shows me who's been giving my address to spammers. But it also means that it's not possible for mail misdirected to my domain to bounce back to the sender as it normally would.

In this case the mail was sent to the right username but the wrong domain (the domain it should have gone to was one letter less than mine). But because I've gotten in the habit of dismissing mail I get with "bogus" addresses as spam, the normal reaction of "I think you goofed your address" was delayed. In this case the ending was happy, but it's easy to imagine somebody never even looking at such mail, with the result that sensitive business negotiations break down, with each side blaming the other for failing to communicate.

Besides the obvious risks of misdirected mail exposing potentially sensitive information to the third parties, another problem is that "convenient" messaging features like blind forwards may make it harder to separate genuine mistakes from games spammers play. The deeper risk is that, as I've seen predicted for some time, the general apathy and distrust that widespread spam has caused are making e-mail less useful as time goes on.

Joe Thompson, Charlottesville, VA joe@orion-com.com
<http://kensey.home.mindspring.com/>

⚡ REVIEW: "The Y2K Survival Guide", Bruce F. Webster

"Rob Slade, doting grandpa of Ryan and Trevor" <rslade@sprint.ca>
Wed, 28 Apr 1999 16:42:55 -0800

BKY2KSUG.RVW 990319

"The Y2K Survival Guide", Bruce F. Webster, 1999, 0-13-021496-5,
U\$19.99/C\$28.95

%A Bruce F. Webster bwebster@bfwa.com
%C One Lake St., Upper Saddle River, NJ 07458
%D 1999
%G 0-13-021496-5
%I Prentice Hall
%O U\$19.99/C\$28.95 +1-201-236-7139 fax: +1-201-236-7131
%P 544 p.
%T "The Y2K Survival Guide"

"Don't buy guns, cash all your stocks, withdraw your savings, and move to South Dakota unless you already had a good reason for doing so, and maybe not even then. It's really cold in South Dakota, and the last place you probably want to be is out in the countryside with a lot of other folks armed with guns and waiting for Armageddon."

While those from South Dakota may bristle a bit at the impugning of their home state, the rest of us may be glad of a little sanity in the year 2000 debate. (On the other hand, maybe the population of South Dakota will be just as glad that someone is telling the nuts to stay home while Ed Yourdon [cf. BKTMBM2K.RVW] is yelling that we're all gonna die. This is, in fact, the book that Yourdon could have written, were he not so busy trying to make application to the Charlton Heston fan club.) (Also, since Webster's roots go 'way back in South Dakota, they'll probably forgive him.) Webster does not so much occupy the middle ground as look at the entire spectrum of reactions to the situation, and tries to remain rational throughout. Whoever did the cover design caught the tone perfectly: an ostrich with its head in the sand in the foreground, and a mushroom cloud in the background. And an awful lot of territory in between.

Part one looks at how we got here. Chapter one starts with an overview of the problem and its cause. Unfortunately, while there are some very good points (such as the statement that it is a century, rather than millennial, problem) the basic explanation is somewhat confused, and doesn't rise above the generally available material on the topic. Whatever faults chapter one may have, though, are more than made up for in chapter two, which gives a clear and almost lyrical description of why the problem happened. Starting with limited hardware, continuing through software bloat, and ending with the seven deadly sins, the lessons are clear and unflinching. (I can even forgive the mention of the scandal du jour, given the deft manner of its inclusion.) A number of the myriad barriers to getting the job done are examined in chapter three. Chapter four reviews a number of myths in regard to Y2K.

Part two looks at preparation in this last year before the deadline. This section is full of suggested actions you can take, to a greater or lesser extent, to get ready. Chapter five looks at laying a foundation: how to plan what to protect. This may seem facile, but it has a real purpose. If you can't do everything, and you probably can't, make sure you do what is most important. To you. Where other books may have a bibliography, chapter six lays out some guidelines for actually getting yourself educated for what might come. The discussion of health ranges from the possible failure of Medicare to starting a fitness program (so as to generally improve your health and

avoid the possibility of hospitalization), in chapter seven.

Chapter

eight reviews planning for home needs. Food concerns, in chapter nine, tend to be weighted towards flour, dried foods, and other items

that need preparation (and therefore, in most people's minds, electricity and water) but the exercise and some pointers are quite

helpful. The "career" plan in chapter ten is probably appropriate to

any situation, quite apart from the possibility of a recession, and

the financial planning in chapter eleven is pretty sound.

Building a

community and support network is possibly the most important thing you

can do to prepare, and is hardly ever mentioned apart from this book's

chapter twelve.

Part three is again preparation, but more of a mental type.

Chapter

thirteen looks at the value (and danger) of trying to see what's ahead. A variety of scenarios, ranging in severity, are presented in

chapter fourteen.

Part four talks about getting on with life after Y2K, and whatever it

brings. Chapter fifteen suggests taking stock and making an assessment. The lessons we should learn from the year 2000 fiasco are

reviewed in chapter sixteen.

Two of the appendices are from work the author did with the Washington, DC Year 2000 Group. Appendix A contains testimony presented to Congress, and Appendix B gives the results of two surveys

of the group members. Appendix C has a very useful set of resources

for further study, heavily weighted to Internet sites.

Like the more sensationally named "Time Bomb 2000" (cf. BKTMBM2K.

RVW),
this book is aimed at the general population. It does a much better job of presenting the reality, and, at the same time, suggesting useful ways to address the issue.

I think it's appropriate to close with another quote from the book,
this one only a few sentences after the one that opened this review:

"Focus on solving as many problems as you can in your own circle of influence, starting with your own life and family, but including your community. Build social cohesion. Do the same sensible personal preparation ..."

copyright Robert M. Slade, 1999 BKY2KSUG.RVW 990319
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

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

⚡ Advanced Workshop: USENIX Smartcard Technology, May 10-11, Chicago

Jennifer Radtke <jennifer@usenix.ORG>
Fri, 30 Apr 1999 00:55:55 GMT

USENIX WORKSHOP ON SMARTCARD TECHNOLOGY
May 10-11, 1999, McCormick Place South, Chicago, Illinois, USA

Review the full program and register on-line at
<http://www.usenix.org/events/smartcard99/>

For Researchers, Product Developers and Smart Card Deployers
First of Its Kind in North America

Sponsored by The USENIX Association

[Abridged for RISKS. PGN]

✉ CFP, 1st European Anti-Malware Conference

<jblaha@nacma.nato.int>

Wed, 28 Apr 1999 07:06:11 +0100

EICAR - European Institute for Computer Anti-Virus Research

March 4 to March

7, 2000, Brussels, Belgium SUBMISSION DEADLINE for PAPERS: JULY
1, 1999

Papers pertaining to malicious code, unwanted side-effects or malfunction, network security, information age and society, cryptography and the protection of privacy and anonymity, new media, and electronic commerce, are welcome. Subject matter may be theoretical, empirical, or methodology oriented. We are interested in receiving Research Papers, Research in Progress Reports, Case Studies and proposals for Symposia. For full details see <http://www.eicar.dk/submit/call.html> or send e-mail to call@eicar.dk

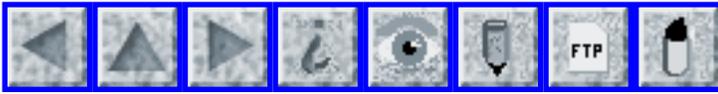
For more information about EICAR please visit <http://www.eicar.org>

JAROSLAV BLAHA, Dipl.Inform.(Univ), Dipl.Wirtschafts-Inform.
(Univ)
Senior Information Systems Engineer

NATO ACCS Management Agency (NACMA), Project Implementation
Division

8, Rue de Geneve, B-1140 Brussels, Tel.: +32-2-707.8540 Fax.:
+32-2-707.8777

jblaha@nacma.nato.int www.jaroblaha.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 20: Issue 36

Saturday 1 May 1999

Contents

- [Seagulls speak English: Aldershot](#)
[John Haseler](#)
- [Yet another satellite hits the dust](#)
[Joan L. Grove Brewer](#)
- [Titan 4B places military satellite in improper orbit](#)
[PGN](#)
- [No Bell Tolls for thee](#)
[Jeremy Ardley](#)
- [Risks of "smart" MS Internet apps](#)
[Andrew Shieh](#)
- [Re: Dodgy automatic address book resolution](#)
[Larry Pryluck](#)
- [MS-Outlook 98 risk of mislaying messages in Outlook today](#)
[Jahn Rentmeister](#)
- [Bloatware and the Windows API](#)
[Diomidis Spinellis](#)
- [Re: The Bloatware Debate](#)
[Henry Baker](#)
- [Bloatware and Nightlight Saving](#)
[R.A. Downes](#)

- [Update on DejaNews click-through monitoring](#)
[Richard M. Smith](#)
 - [Re: WC Watch Company site ...](#)
[David B. Horvath](#)
 - [Re: Risks of misaddressed mail](#)
[Frederick M Avolio](#)
 - [REVIEW: "A Guide to Virtual Private Networks", Martin W. Murhann](#)
[Rob Slade](#)
 - [CONF: 12th Software Quality Week](#)
[Software Research](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Seagulls speak English: Aldershot

"John.Haseler@bcs.org.uk" <John@haseler.demon.co.uk>

Sat, 1 May 1999 23:30:44 +0100

Quote from **Daily Telegraph**, 1 May 1999, Property section - in an article explaining how to keep seagulls from nesting on your chimney-stack:

The other day, I got a call from a man complaining that the gulls outside his window were interfering with his voice-activated computer.

Apparently, every time a seagull let out a loud squawk, his computer

would type up the word 'Aldershot' on this screen. After a while,

that kind of thing can drive you mad.

[I guess the computer software was gulled into a characteristic

AI pattern mismatch. But this is clearly worth some further study.

What would one good tern turn into? Gullible's Travels?

And what is the domain of discourse that includes Aldershot? PGN]

⚡ Yet another satellite hits the dust

"Joan L. Grove Brewer" <pegasus@transport.com>

Sat, 1 May 1999 02:40:30 -0700

On 28 Apr 1999 the *Seattle Times* and other new media reported that yet another satellite had mysteriously lost contact.

http://www.seattletimes.com/news/nation-world/html98/altsate_19990428.html

In the article -- A real-life X-Files case: Where's the satellite?

-- John Antczak of The Associated Press

"Ikonos 1 (Greek for image) disappeared yesterday almost immediately after it was launched from California's coast."

It was going to be only a 400-mile-high orbit, and they are puzzling over what could have gone wrong... This was the first private satellite that could take high resolution images of earth. ONLY the military could do this until now. [In 1994, the U.S. Government authorized Space Imaging to launch a private satellite. PGN]

There is still that BIG PUZZLE about what happened. In fact, there have been so many problems with private satellites that it does in fact beg the question... Is this an X-File? :-) or is this something else. So many satellites have been messing up that last weeks Dilbert TV show which aired

on April 26 they did a bit on satellites. Dilbert messed up and a satellite went out of orbit hit another satellite and they all went so nuts that the whole world shut down... It was really quite funny. Then bingo, two days later yet another satellite bites the dust--perhaps literally.

Craig McCaw and Bill Gates put together a company called Teledesic that was originally going to put 840 satellites in low orbits until Boeing talked the down to 280. I wonder what their game score will be. Boeing who is doing the project with them had one of the rocket blow up on the pad as well as their satellite. :-) This could really get to be quite an expensive business, especially if it's due to a natural phenomena like radiation belts or a new sun cycle with massive sun spots. Maybe it will eventually get turned back on.

Could this just be due to human error. Low Orbiting satellites have to be piloted by humans. My original concern to the boys was where are you going to find the highly trained and skilled engineers to run that many satellites. We can't even find people to operate our computer systems and the Internet? This is what I think the real problem is. It's like with our older mainframes having to have system engineers sleeping on cots in the back room to baby sit all the time... Now with a lot of people raised on computers do we really have the brain power to react fast enough in a crisis situation?

Joan Brewer -- retired systems engineer

✦ Titan 4B places military satellite in improper orbit

RISKS List Owner <risiko@csl.sri.com>

Sat, 1 May 99 10:39:45 PDT

The U.S. Air Force is on another rough road in the sky.

A Titan 4B rocket (cost about \$433.1 million) was launched from Cape Canaveral on 30 Apr 1999 carrying a Milstar military satellite (worth about \$800 million). Both were built by Lockheed Martin. The three firings of the Centaur upper-stage booster apparently occurred prematurely, resulting into the satellite separating four hours early into an elliptical orbit from 460 miles to 3,105 miles up, rather than the intended stationary geocentric orbit at 22,300 miles above the equator.

This was the third failure in a row -- following the Titan 4A with a Vortex satellite last August 1998 in a mission with comparable costs ([RISKS-19.91](#)), and a missile warning satellite on 9 Apr 1999 stuck in a useless orbit.

✦ No Bell Tolls for thee

"J&J Ardley" <jardley@ibm.net>

Sat, 1 May 1999 20:07:05 +0800

The following text is part of

<http://www.microsoft.com/security/resources/NATOCaseStudy.asp>

dated

February 1999 as an example of a high security implementation of NT for military purposes. The CRONOS system is a wide area network of NT computers used in NATO in Europe in the present conflict in the Balkans. Steakley is David Steakley, Cronos Project Leader at NC3A. Jeremy Ardley

Quote:

Security of Windows NT Crucial to Cronos Because Cronos carries classified information, security was a top requirement. Specifically, NATO regulations required that Cronos use an operating system that carried the imprimatur of an independent security evaluation. "We had to have assurance that security rules could be enforced-to make sure that when anyone logs onto the system, he is authorized to log on and has security clearance at the level the system requires," says Steakley.

"We insist that all of our systems meet the C2 level of security when they're used for classified information, on both the client and the servers," says Steakley, referring to a security rating level in the US

Government's Trusted Computer Security Evaluation Criteria. Windows NT 3.5

has been successfully evaluated by the US Government at the C2 level and

Windows NT 3.51 has been successfully evaluated by the UK Government at a comparable level of E3/FC-2. Because of this lineage and the fact that

Windows NT 4.0 had been submitted for its own C2 evaluation, Windows NT

4.0 met NATO's security requirements."

In contrast to this is the following from

<http://www.gcn.com/gcn/1998/October26/8.htm> dated October 26, 1998 which includes

Quote :

NT 4.0 is not certified at the C2 level by NSA. Microsoft, however, is in the process of getting C2 certification for NT 4.0 with Service Pack 4 in a closed network configuration.

The essential element is that C2 certification to date applies to non-networked configurations of NT 3.51 on a specific set of hardware.

Clearly the client and server configuration of NT 4.0 referred to by Steakley are not covered by the existing C2 certification. Extrapolation by Steakley of the certification of 3.51 to 4.0 is also a non-sequitur, especially as he claims that submission for evaluation equates to granting of a certificate. Under his logic I should claim a Nobel prize when I next submit my name to the committee.

⚡ Risks of "smart" MS Internet apps

andrew shieh <shandrew+usenet.mil.gov@leland.Stanford.EDU>
Sat, 1 May 1999 01:41:19 -0700

Recently, in response to a simple question about perl, i posted the answer of:

```
//i
```

This worked fine. The person who i was responding to was using Microsoft

Outlook Express to read the newsgroup. He couldn't seem to figure out what that meant. He quoted my message, and the "//i" showed up as "file://i", and i guessed that that was how it also appeared to him on screen.

What you get is not what you see.

✶ Re: Dodgy automatic address book resolution (Liddicott, [RISKS-20.34](#))

"Pryluck, Larry" <PryluckL@issc.belvoir.army.mil>

Thu, 29 Apr 1999 12:38:41 -0400

I had an experience similar to Samuel Liddicott's. Our office uses MSExchange 5.0 running on Windows NT Workstation 4.0. I tried to forward a leave form to our secretary, Ann Jack, who's e-mail address is resolved on the Global Address List. I was chagrined to find out a day or two later that the mail went instead to my friends Jack and Anne, whose e-mail address is in my personal address book, which is first on the list. This was even after selecting "Ann Jack" from the global address list. I may have even put in the address to the right of the @ as well.

I finally gave in to the dark side and made "AJ" an entry in my personal book. No problems now, but it continues to amaze me how what used to be a simple thing has been made complex by software that tries to out think the user.

Larry Pryluck, US Army Information Systems Software Center

✶ MS-Outlook 98 risk of mislaying messages in Outlook today

Jahn Rentmeister <rentmei@uni-muenster.de>

Mon, 26 Apr 1999 18:32:43 +0200 (MES)

MS-Outlook as an MS-Exchange client uses a hierarchical folder list to store e-mail messages in. Folders can contain mail messages, but also other folders. The top-level folder is the "mailbox", which contains, among other folders, a folder for incoming mail.

In Outlook 97, the top-level folder is just a folder like any other, in particular, it can contain folders and mail messages, and activating the folder shows its contents. In Outlook 98, however, displaying the top-level folder of a mailbox displays an "Outlook today" screen, featuring "links" to the user's calendar, task lists, e-mail drafts and inbox as well as a search facility. However, the contents of the folder are not displayed in Outlook 98. But it is still possible to move e-mail messages into that folder.

This creates a situation where it is possible for a user to move a message to that folder, but is later unable to access that message. (Unless the e-mail message is found by a search of all folders.)

Moving messages into folders is commonly done with the mouse, and accidentally moving messages to the wrong destination folder is not uncommon (at least not for me). This can create (and has created)

situations where
e-mail messages "magically" disappear, possibly before they have
been acted
upon or even before they have been read.

To my knowledge, there is no way accessible to the average user
to check the
contents of this folder in Outlook 98, or to disable the
"Outlook today"
display.

The fact that contents of the folder are not displayed together
with
the "Outlook today" screen is not obvious to the user, except if
a
user tests this by deliberately moving mail into that folder.

This "feature" was not present in Outlook 97, and it is possible
to check
the folder contents using Outlook 97. (With MS-Exchange, e-mail
messages and
folder structure are usually stored on the server)

There is a way to disable the "outlook today" feature, described
at
<http://support.microsoft.com/support/kb/articles/q184/8/56.asp>
(create and set a special key in the Windows registry)

Jahn Rentmeister <rentmei@uni-muenster.de>

Bloatware and the Windows API

Diomidis Spinellis <dspin@aegean.gr>
Sat, 01 May 1999 15:19:23 +0300

A number of contributors to previous digests have stressed the
risks
associated with increasingly bloated software applications. I
believe that

a part to the complexity and unreliability of many modern software applications can be attributed to their use of the Windows Application Programming Interface (API).

I recently wanted to read - using C code - the name of the file pointed by a Windows shortcut: a shell-level equivalent of the Unix symbolic link. Unix symbolic links can be read by using `readlink(2)` - a simple three argument system call. The code I had to write to examine the Windows shortcut spanned over 100 lines of C and included initialisation of the COM (component-object model) library, checking for Unicode filenames, getting pointers to two COM interfaces, and releasing all the associated handles at the end. Seven of the API functions could return with an error which had to be checked. I am sure other readers can point to other similar examples.

The architecture, interface, and functionality of the Windows API make it difficult to master and use effectively, and contribute negatively to the safety, robustness, and portability of the applications developed under it. The API is structured around a large and constantly evolving set of functions and is based on a problematic shared library implementation (the infamous Dynamic Link Libraries - DLLs). The provided interfaces are complicated, non-orthogonal, abuse the type system, cause namespace pollution, and use inconsistent naming conventions. In addition, the functionality of the interface suffers from inconsistency, incompleteness,

and inadequate documentation [1].

I foresee that problems associated with the use or misuse of the Windows API will provide material for many future RISKS digests.

[1] Diomidis Spinellis. A critique of the Windows application programming interface. *Computer Standards & Interfaces*, 20:1-8, November 1998.

<http://kerkis.math.aegean.gr/~dspin/pubs/jrnl/1997-CSI-WinApi/html/win.html>

Diomidis Spinellis, University of the Aegean

✉ Re: The Bloatware Debate (Downes, [RISKS-20.35](#))

Henry Baker <hbaker@netcom.com>

Sat, 01 May 1999 06:51:36 -0700

> One of the chief hallmarks of early UNIX was how simple, compact programs
> worked well together....

The biggest productivity losses due to bloatware are IMHO the enormous

intellectual effort of the compiler people to 'optimize' bad code into good code, and of the CPU hardware architects to make 'legacy' bad code run fast.

I would estimate that 50-70% of the size of compilers and 50-70% of the size of CPU chips is devoted to protecting the investment in code that never should have seen the light of day.

On another note, though, Unix itself inspired a generation of programmers to write bad, buggy code that never bothered to check error codes,

and assumed
that all input was error-free. There was a wonderful paper in
the
Communications of the ACM a number of years ago about feeding
'line noise'
into various standard (and presumably well-debugged) Unix
utilities and
seeing the spectacular crashes that ensued.

✶ Bloatware and Nightlight Saving

<main@radsoft.net>

Sat, 01 May 1999 07:58:09 +0000

While we're on the bloatware debate, let's look at some
wonderful features
that have come our way via that Mecca of intellectual happiness,
Redmond
Washington.

The incident below takes place soon after the Premium Release of
Windows 95
and about one week before my corporation scrapped it altogether.
I had 95
installed in my home and it was Saturday night and time for
bed. I kicked
in the screen saver and joined my wife under the covers.

Some hours later I was wakened from a sound sleep by a commotion
in the next
room. The wife did not wake, but I did, and I was curious what
had cause the
noise and went in to check.

It was the computer. The monitor screen had a big message box
planted on
it. The wording was something to the effect:

"Microsoft Window 95 has detected that you have now gone over to
standard

time from daylight savings time and has adjusted your computer's clock accordingly. Thank you for choosing Microsoft Windows 95."

I was impressed! When I returned to bed the wife was stirring and protesting my being up and about. I told her "you'll never believe what that Bill Gates did now!" and as she drifted off again to sleep I gave her the whole story.

But my sleep and mirth with Microsoft did not last long. It was exactly one hour later that I was awakened again - and for the same reason! The computer's clock, put back from 3 AM to 2 AM by Wonderful Windows, had again hit 3 AM, and - you guessed it - Wonderful Windows again put it back to standard time. At this rate Sunday would never occur!

Even though I knew better I passed it off as a fluke and went back to bed. And both one hour later and two hours later (my time, not Microsoft's) I was rudely disturbed by the collective alternative intelligence of Redmond. At that point I turned the machine off, had a few moments of black insight into how things are done and tested in that cauldron of cerebral superiority, and decided then and there that Microsoft Windows 95 could never be taken seriously.

RA Downes Radsoft Laboratories <http://www.radsoft.net>

🔥 Update on DejaNews click-through monitoring

"Richard M. Smith" <rms@pharlap.com>

Sat, 01 May 1999 17:23:26 -0400

I just wanted to give an update on the DejaNews ruckus that got started in the comp.security.misc, alt.privacy, and comp.risks newsgroups earlier this week.

As reported by myself and a number of other folks, DejaNews is monitoring when people click on links to external Web sites and e-mail addresses in newsgroup messages displayed by DejaNews.

DejaNews issued a statement on Friday afternoon saying that they plan to stop monitoring click-throughs of e-mail addresses.

ComputerWorld and

Wired both have stories on this announcement:

<http://www.computerworld.com/home/news.nsf/all/9904305dejaneews>

<http://www.wired.com/news/news/politics/story/19435.html>

This is good news, as there was no particular reason in the first place for DejaNews doing this sort of thing. The software changes on the DejaNews servers should be pretty trivial to make.

According to *ComputerWorld*, DejaNews may continue to track when people click on a link to external Web site in a newsgroup message. This is somewhat of an unusual practice for a search engine to be doing. To my knowledge only Hotbot does this same sort of tracking. For people concerned about this, a simple solution is to copy the link text and paste it into the location or address window of a browser. This solution bypasses the redirect trick being used by the server to do the monitoring.

The larger issue that I see here is something that can affect

any Web site

or ISP. The more information that a Web site or ISP chooses to track and save away, the more likely they are to be dragged into legal disputes.

Lawyers and law enforcement people are increasingly asking for and getting log files from both ISP and Web site operators. Here are some interesting articles on this subject:

"Arrest made in Bloomberg story hoax"

<http://www.news.com/News/Item/0,4,35201,00.html>

"Internet chat faces new suit"

http://www.boston.com/dailyglobe2/119/business/Internet_chat_faces_new_suit+.shtml

"Spouses may delete their marriage, but e-mail lives on as evidence"

[http://archives.seattletimes.com/cgi-bin/taxis.mummy/web/vortex/display?stor](http://archives.seattletimes.com/cgi-bin/taxis.mummy/web/vortex/display?storyID=372780441&query=divorce)
[yID=372780441&query=divorce](http://archives.seattletimes.com/cgi-bin/taxis.mummy/web/vortex/display?storyID=372780441&query=divorce)

"Online, both the guilty and innocent are easy to spy"

[http://www.boston.com/dailynews2/120/economy/Online_both_the_guilty_and in:.shtml](http://www.boston.com/dailynews2/120/economy/Online_both_the_guilty_and_in:.shtml)

Things will get really interesting if information from server logs is turned over in a civil case about some individual and this individual thinks that the Web site operator or ISP shouldn't have been collecting and archiving the information in the first place.

Richard M. Smith <smiths@tiac.net>

⚡ Re: WC Watch Company site ... (Ziglar, [RISKS-20.35](#))

David B. Horvath, CCP <dhorvath@cobs.com>

Fri, 30 Apr 1999 21:58:58 -0400 (EDT)

>IWC, a Swiss manufacturer of high-end wristwatches, ...

Ahh, the risks of common TLA domains. www.iwc.com is InLink Web Creations (actually refreshes to www.inlink.com - Inlink Communications, an ISP in St Louis).

<http://www.iwc.ch> gets you the watch manufacturer. There were three people listed: "Mrs. Privacy Invasion (anon@127.0.0.1)", "Mr. up (yours)", and "Mr. Prinya Sivasirikarul (no e-mail address)". I wonder if Mrs. Invasion reads RISK Digest?

David B. Horvath, CCP dhorvath@cobs.com
Consultant, Author, International Lecturer, Adjunct Professor

[Also noted by Mike Durkin. But it seems people are not necessarily giving the requested information. That seems like a very good idea, although may not be good enough. PGN]

⚡ Re: Risks of misaddressed mail (Thompson, [RISKS-20.35](#))

Frederick M Avolio <fred@avolio.com>

Fri, 30 Apr 1999 19:22:33 -0400

The bigger problem, and I think more problematic, is our total dependence on

e-mail when a telephone call could clear things up nicely. We assume because e-mail almost always works, that it **will**. Sometimes a telephone call to clear things up or to inquire as to status will save days of time and e-mail. I suspect we have all been in exchanges of e-mail that would have beeter and more quickly been done via the telephone.

I love e-mail. Love using it. I believe I fully understand and appreciate its utility. But it is not the ultimate communication tool. Sometimes a call, "did you ever send that document to me?" saves time and effort.

Fred, Avolio Consulting, 16228 Frederick Road, PO Box 609,
Lisbon, MD 21765
410-309-6910 (voice) 410-309-6911 (fax) <http://www.avolio.com/>

⚡ REVIEW: "A Guide to Virtual Private Networks", Martin W. Murhamm

Rob Slade <rslade@sprint.ca>
Fri, 30 Apr 1999 08:20:06 -0800

BKAGTVPN.RVW 990321

"A Guide to Virtual Private Networks", Martin W. Murhammer et al,
1998, 0-13-083964-7

%A Martin W. Murhammer

%A Tim A. Bourne

%A Tamas Gaidosch

%A Charles Kunzinger

%A Laura Rademacher

%A Andreas Weinfurter

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

%D 1998

%G 0-13-083964-7
%I Prentice Hall
%O 800-576-3800 416-293-3621 fax: 201-236-7131
%P 174 p.
%T "A Guide to Virtual Private Networks"

You don't have to look very far to figure out that this book is by IBM, of IBM, and probably for IBM. All of the authors (even those that don't rate the front cover) work for IBM, and ... well, lookee here! IBM just happens to make products that relate to virtual private networks (VPNs)!

Chapter one is a reasonable overview of the basic concepts behind VPNs. However, the level of the writing is inconsistent, some parts of the explanation are a bit confused (they tend to use the term "tunnel" a lot, even where "circuit" might be more fitting), and overall one gets the feeling that this should be presented on a big screen in a dark auditorium, with a suit droning on and on. There is a tendency to illustrate (with not very illuminating figures) rather than explain, when it comes to the technical bits. Either that, or just start to list off protocols.

Encryption is explained fairly well in chapter two. There is some detail as to the actual operation of some algorithms. (I notice that DES [Data Encryption Standard] is not among them, and that it is claimed fully, and not just derivatively, for IBM.) The discussion of key and algorithm strength is weak, however, and there is no discussion of the basic problems or concerns of key management.

Chapter three provides format details of the IPsec (Internet Protocol security) AH (Authentication Header) and ESP (Encapsulating

Security

Payload) protocols. References for the appropriate draft documents are given at the end of the chapter. The Internet Key Exchange (IKE) (also known as Internet Security Association and Key Management Protocol [ISAKMP]) is discussed in chapter four. Chapters five to seven look at scenarios for branch offices, business partners, and remote access, respectively. There is little new content, and most of the material could be inferred from the text of earlier chapters. Showing admirable forbearance, most of the detail of IBM products is held for the appendices.

While not all parts are particularly readable, the book does, at least, have the advantage of being short. The fundamental concepts of VPNs are given, enough so that a technical manager could get a basic grasp of what was required. Possible attacks, and the complexities of implementation, are not dealt with very well.

copyright Robert M. Slade, 1999 BKAGTVPN.RVW 990321
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

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

⚡ CONF: 12th Software Quality Week (QW'99; edited for RISKS)

Software Research <sr@netcom.com>

Fri, 30 Apr 1999 20:25:40 GMT

The 12th Annual International Software Quality Week (QW'99) will be held

26-28 May 1999 in San Jose, California USA. Two days of pre-conference tutorials are 24-25 May 1999. The complete program for QW'99 can be found at the QW'99 Conference WebSite:

<<http://www.soft.com/QualWeek/QW99>>

KEYNOTE SPEAKERS (26-28 May 1999) address the Conference Theme "Facing the Future" in a coordinated sequence of talks:

- * Martin Pol (IQIIP Informatica BV) "Facing the Future Means Facing Test Maturity"
- * Jeff Schuster (Rational) "Facing the Future: E-Commerce Quality and YOU!"
- * Cem Kaner (Attorney at Law) "Facing the Future: The Law"
- * Roger Sherman (Independent Consultant) "Facing the Future: Commercial Product Testing"
- * Jakob Nielsen (Nielsen Norman Group) "Facing the Future: Usability Aspects of Quality"
- * Brian Marick (RST) "Facing the Future: New Models for Test Development"
- * Boris Beizer (Independent Consultant) "The Mavin"

COMPLETE INFORMATION or to register by phone or by mail is available from:

SR/Institute
901 Minnesota Street
San Francisco, CA 94107 USA
Phone: +1 (800) 942-SOFT (7638) or +1 (415) 947-1441
FAX: +1 (415) 957-0730
E-Mail: qw@soft.com
Web: <<http://www.soft.com/QualWeek/QW99>>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 37

Tuesday 4 May 1999

Contents

- [Revisiting the USS Yorktown dead in the water](#)
[Mike Martin](#)
- [Netfill scams 900,000 credit cards](#)
[PGN](#)
- [Australian Securities & Investment Commission's April Foolery](#)
[Pauline van Winsen](#)
- [Re: Bloatware Debate](#)
[RA Downes](#)
[Jonathan Goldberg](#)
[Henry Baker](#)
[RA Downes](#)
- [Interesting results with MapQuest](#)
[Matthew Delaney](#)
- [New risk of ITAR?](#)
[David Leshner](#)
- [Risks of "Discovery" hounds](#)
[Russ Cooper](#)
- [Outdated address books](#)
[Robert David Graham](#)
- [Israeli scientist reports discovery of advance in code breaking](#)
[Edupage](#)

- [Re: CIH virus](#)
[Matthew Todd](#)
 - [Re: MS-Outlook 98 risk of mislaying messages in Outlook today](#)
[Jedediah Grant](#)
 - [Smart Card Forum Privacy Symposium, 20 May 1999](#)
[Donna Farmer](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ Revisiting the USS Yorktown dead in the water (PGN, [RISKS-19.88 ff.](#))

"Martin, Mike" <mmartin@sbns.com.au>

Tue, 4 May 1999 17:26:00 +1000

The RISKS discussion related to a zero-divide in an NT application on a Navy ship, that crippled the ship for some time.

Scientific American finally caught up with the topic in November 1998

(www.sciam.com/1998/1198issue/1198techbus2.html), although the report added

little new to what has appeared already in RISKS. Then in the March 1999

issue (which I have just received) there is a letter from Harvey McKelvey,

former director of Navy programs for CAE Electronics, the firm which

apparently built the misbehaving application

(www.sciam.com/1999/0399issue/0399letters.html).

McKelvey writes that the failure, "was not the result of any system software

or design deficiency but rather a decision to allow the ship to manipulate

the software to stimulate [sic] machinery casualties for training purposes

and the 'tuning' of propulsion machinery operating parameters.

In the usual
shipboard installation, this capability is not allowed."

McKelvey adds that CAE Electronics expressed "serious concern"
when this
test was proposed.

So it seems that as long as there are no "machinery casualties",
everything
will be fine. Then again, the incident may have provided useful
information
to improve system robustness.

Mike Martin <mmartin@sbns.com.au>

⚡ Netfill scams 900,000 credit cards

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

Tue, 4 May 99 8:39:45 PDT

Netfill, which provides access to pornographic Web sites, has
apparently
billed something like 900,000 credit-card numbers for services.
Federal
regulators claim that the owner, Kenneth H. Taves, has been
squirreling
millions of dollars in offshore banks. FTC officials have not
yet
determined how the numbers were acquired -- perhaps he may have
used a
"number generating program"! [Source: *San Francisco
Chronicle*, 4 May
1999, A3]

⚡ Australian Securities & Investment Commission's April Foolery

Pauline van Winsen <Pauline.van.Winsen@eserv.com.au>

Tue, 4 May 1999 08:38:02 +1000 (EST)

The Australian Securities & Investment Commission created a hoax Web site:

<http://www.smbi.com.au> on April 1st this year. The site boasted that punters would triple their money if they invested their money in Millennium Bug Insurance. The site attracted \$4 million worth of interest from people who were fooled by the web site. Only a few alerted ASIC that the company didn't seem legit. The site was designed to educate the public about the risks of investing in Internet ventures.

Full Story at:

<http://www.theaustralian.com.au/index.asp?URL=/national/4291177.htm>

Pauline van Winsen, Senior Technical Consultant

pauline@eserv.com.au

eServ Pty Ltd

[http://www.eserv.com.au/people/](http://www.eserv.com.au/people/pauline.html)

[pauline.html](http://www.eserv.com.au/people/pauline.html)

[Ah, yes, the adage seems to be,
"If it has to do with the Internet,
it must be worth investing in." PGN]

⚡ Re: Bloatware Debate (Downes, [RISKS-20.35](#))

RA Downes <main@radsoft.net>

Sun, 02 May 1999 16:12:13 +0000

A certain "Johnny" has written to me from Microsoft because of my posting in [RISKS-20.35](#) about MS bloat. The tone was a thinly disguised threat. In his

opening, "Johnny" stated that the "bloat" of MS RegClean was due no doubt to having static links. Discussing the sweeping ramifications of such a statement is unnecessary here. The mind boggles, it is sufficient to state. The MSVC runtime is a mere 250,000 bytes and in fact is not statically linked anyway to MS RegClean, AFAIK [as far as I know]. MS RegClean is an MFC app and will by default use the dynamically linked MFC libraries. And even if its static code links were an overhead here they would add but a small fraction of the total bloat, say 40KB at most.

For whatever reason, I decided to download the latest version of MS RegClean from BHS again and pluck it apart. This is what I found. I have tried - and it has been difficult - to keep subjective comments out of this report.

Current Status of RegClean Version 4.1a Build 7364.1

=====

Image Size (Unzipped and ready to run): 837,632 bytes (818KB)

=====

(Subjective comment removed.)

Import Tables

=====

The import section in the PE header. This gives an indication of just how (in)effective the use of Bjarne's C++ has been. In this case, the verdict is: "pretty horrible". A whopping 7,680 bytes are used for the names of the relocatable Win32 imports. These are the actual names of the functions (supposedly) called. MS RegClean does not call most of

these functions - they remain because an MFC template was originally used, most likely borrowed from another application, and it was never "cleaned". This is corroborated by what is found among the "Windows resources": over half a dozen standard menus, assorted graphic images, print preview resources, etc. that have nothing to do with the application at hand.

Resources

=====

Please understand that resources not only bloat an executable with their own size, but with additional reference data, in other words the bloat factor of an unused or bad resource is always somewhat larger than the size of the bloating resource itself.

Accelerators

=====

Sixteen (16) unused accelerators from an MFC template were found: Copy, New, Open, Print, Save, Paste, "Old Undo", "Old Cut", Help, Context Help, "Old Copy", "Old Insert", Cut, Undo, Page Up, Page Down. MS RegClean uses only one accelerator itself, not listed here.

Bitmaps

=====

This was a particularly sorry lot. The main bloat here was a splash screen bitmap weighing in (no RLE compression of course) at over 150KB. Further, Ctl32 static library bitmaps were found, meaning MS RegClean is still linking with the old Ctl32v2 static library which was obsolete five years ago and which automatically adds another 41KB to the image size.

Cursors

=====

Six (6) cursors were found, none of which have anything to do with this application.

Dialogs

=====

A very messy chapter indeed. MS RegClean walks around with eighteen (18) hidden dialogs, of which only one or at the most two are ever used. The others are just - you took the words out of my mouth - junk. The findings (read it and weep):

*) Eleven (11) empty dialogs with the caption "My Page" and the static text "Todo", all identical, all empty, and of course all unused. This is a wonder in and of itself.

*) The main "wizard" dialog actually used by the application is left with comment fields to help the programmers reference the right controls in their code (subjective comment removed).

*) A "RegClean Options" dialog which AFAIK is never used.

*) A "New (Resource)" dialog, probably a part of the development process, just stuffed in the stomach at sew-up time and left there for posterity.

*) A "Printing in Progress" dialog.

*) A "Print Preview" control bar dialog.

Icons

=====

MS RegClean has three icons, all with images of 48x48 in 256 colors (of course). The funniest thing here is that the authors of MS RegClean have extracted the default desktop icon from shell32.dll, which is available at runtime as a resident resource anyway and at no image bloat

overhead
at all, and included it in toto in their executable.

Menus

=====

MS RegClean has eight (8) menus, at least half of these are simply junk left around by the MFC template. Another menu indicates that the authors of RegClean have in fact worked from an internal Microsoft Registry tool - rather bloated in itself it seems.

String Table(s)

=====

Actually it need only be one string table, but Microsoft itself has never learned this. The findings here were atrocious. And you must remember that strings stored in a string table are stored in Unicode, which means that their bloat automatically doubles. Further, MS's way of indexing strings in a string table means a 512 byte header block must be created for every string grouping, and strings are grouped according to the high 12 bits of their numerical identifiers (yes they are 16-bit WORD identifiers). Meaning indiscriminate or random numbering of string table entries will make an otherwise innocent application literally explode.

347 (three hundred forty seven, yep, your video driver is not playing tricks on you) string table entries were found in MS RegClean, including 16 identical string entries with the MS classic "Open this document" as well as archaic MFC template toggle keys texts which are not used here

(or almost anywhere else today). Most of these strings have - of course
- nothing to do with the application at hand.

Toolbars

=====

Toolbars are a funny MS way of looking at glyph bitmaps for use in toolbar controls. MS RegClean has two - one which may be used by the application, and one which was part of the original MFC template and never removed.

Total Accountable Resource Bloat

=====

The total accountable (i.e. what can be directly calculated at this stage) resource bloat of MS RegClean 4.1a Build 7364.1 is over 360,000 bytes (350KB).

Total Accountable Code Bloat

=====

Harder to estimate, but considering that most of the code is never used, only part of an MFC template that the authors of MS RegClean lack the wherewithal to remove, the original estimate of a total necessary image size of 45KB for the entire application must still stand.

In Conclusion

=====

Bloat is not a technical issue, but verily a way of thinking, a "state of mind". Its cure is a simple refusal to accept, and a well directed, resounding "clean up your act and clean up your code!"

PS. Send feedback on RegClean to regclean@microsoft.com

RA Downes, Radsoft Laboratories <http://www.radsoft.net>

⚡ Re: The Bloatware Debate

<Jonathan_Goldberg@mastercard.com>

Mon, 3 May 1999 16:47:29 -0500

People seem to be talking about this as the result of mental aberrations common in Redmond. I think that this misses the point. Bloated software is the predictable result of the incentives operating in the software industry. In part, this is a perfectly rational use of resources. Code compactness, like any other desirable engineering outcome, must be traded off against things such as cost and time to market. As hardware gets cheaper relative to programmer time, it is reasonable to use more hardware and less programming effort. Microsoft's monopoly exacerbates this tendency. As long as they can annoy people into buying their software because there is no viable alternative (taking into account factors such as training costs, interoperability, and the Company approved software list), Microsoft faces the tradeoff of spending their money on compact code or your money on hardware. It's not a hard choice.

⚡ Re: The Bloatware Debate (Downes, [RISKS-19.35](#))

Henry Baker <hbaker@netcom.com>

Mon, 03 May 1999 15:24:14 -0700

> One of the chief hallmarks of early UNIX was how simple,
compact programs
> worked well together....

To better understand bloatware, we may have to look to evolutionary biology. For example, peacocks have enormous tails and deer have antlers that certainly can't be explained by the usual 'survival of the fittest' kinds of arguments. The prodigious amount of energy required to grow these appendages has to reduce the animal's ability to run away from danger or survive an extended lack of food. Matt Ridley's 1993 book "The Red Queen" (ISBN 0-14-016772-2) is an outstanding discussion of the new thinking about such things in the field of biology.

According to a Red Queen type of argument, bloatware will survive precisely because it is bloatware_ -- the bloat is a kind of 'display' similar to peacock tails or antlers used to prove the vigor of its creator, as only a truly vigorous creator could afford to waste the prodigious sums required to implement gross and useless appendages like 'Clippy'.

✶ Re: Bloatware Debate

RA Downes <main@radsoft.net>
Mon, 03 May 1999 01:46:36 +0000

Bloatware is something we are very sensitized to here. The way we see it, there is no excuse, because there is no reason.

I personally accepted Brian W. Kernighan's calculations back in the old days about a 10% bloat with C versus assembler because the rewards were tangible and far outweighed the bloat: you got largely (according to Steve Johnson 94%) platform independent code, saving countless man-hours of work.

But ever since the popular inception of MS Windows and furthermore MS's MFC things have been way out of control. This is partly due to C++ and partly, if not largely, due to MS and their MFC itself. A typical Win16 application was 5KB, yet the same skeleton if built with the MFC back then was ten times that size. And Bjarne's words echoed in your ear: "C++ produces no noticeable overhead versus C." It simply was not so, and never will be so.

With time the MFC overhead has been reduced somewhat, but programmers of today, raised on OO and C++ as opposed to what others have gone through, are simply not taught to be conservative and minimalistic.

I received a letter yesterday from someone who had been reading the Risks Digest, and reported on a party he had attended some years earlier. The conversation turned inevitably toward software, and he mentioned that he often must really tweak code to get it compact and fast. Another person at the party, from you guessed it Redmond Washington, said that was *not* the way things were done there; she said that if they ever ran into performance problems, they just "threw more hardware at it."

So there are several issues involved all at once, and AFAIK the only way to fight this, for stop it we must, is to expose it and make even ordinary end users understand what it's all about, and perhaps by a concerted effort we can turn back the tide.

Rick Downes, Radsoft Laboratories <http://www.radsoft.net>

✶ Interesting results with MapQuest

Matthew Delaney <delaney@ucs.net>

Mon, 03 May 1999 01:49:46 -0400

I was recently searching for a road in Albany, NY (USA). I went to MapQuest (www.mapquest.com) as I often do when searching for an address. I entered, in the address field, "Route 85" and then Albany and NY in the city and state fields. Knowing this is an actual road, and having seen it on MapQuest Albany maps before, I expected MapQuest to locate it. However, it returned "Address: 85 Rita Ln Albany NY 12211-2321 US." I repeated this same request several times, to the same result. Even more interesting, when I started clicking around the map or changing my zoom level, the top of the map displays "Your search origin is: Route 85, Albany, NY, US."

Obviously MapQuest is attempting to make a guess on my request, and in this case, getting it very wrong. Normally if it can not find the address you request, it tells you so at the top of the map and then normally displays a

city level map. However, in this case, it made no indication that it was making a guess.

Just because data is returned, it isn't necessarily what you expect it is.

Matthew Delaney <delaney@ucs.net>

⚡ New risk of ITAR?

David Leshner <wb8foz@nrk.com>

Sat, 1 May 1999 22:48:35 -0400 (EDT)

<http://www.washingtonpost.com/wp-srv/WPlate/1999-05/01/1691-050199-idx.html>

Serbs Listening In on Pilots:

Some Attacks Thwarted Because of Allied Jets' Unsecure Radio Gear

By Dana Priest, *The Washington Post*, 1 May 1999; Page A01

Yugoslav forces have apparently thwarted some NATO air attacks because

at times allied pilots speak to each other and to ground-based air

controllers over open communications systems, according to NATO

officials and U.S. intelligence reports ...

OOPS! It seems as if not all NATO members *have* interoperable voice-encryption gear in their aircraft...

The RISK? Law of Unintended Consequences, maybe? Sometimes suppressing an export market for 1979 reasons bites you on the backside in 1999...

Can PGPphone work on a CRM-114, maybe?

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

⚡ Risks of "Discovery" hounds

Russ <Russ.Cooper@rc.on.ca>

Mon, 3 May 1999 13:44:09 -0400

May 3rd, numerous sources published a link to what they believed was Microsoft Windows NT 4.0 Service Pack 5. SP5 represents a return to service packs every 6 months from Microsoft after SP4 took nearly 18 months to get released.

Unfortunately, for some, it turned out that the publicly accessible file was actually a Release Candidate version of SP5, and not the Final RTM version. Microsoft's web release mechanisms are, well, in flux right now and often take longer than people expect. As such, various components of such a release are often put in place before others. In this case, the 32MB self-extracting zip file of the SP RC was likely placed in a public location to verify, privately, that beta testers could actually access it correctly via the public site. For such a test, there's no need to ensure the file is the final RTM, just use what's at hand.

Despite no public acknowledgement from Microsoft, and despite the Windows NT Downloads Home Page still featuring SP4 as its "featured download", a few, probably, well intentioned soles started sending notes to various lists and

posting the link on their home page as "SP5 RTM".

Likely an age old risk, the issue of "official" information. As the moderator of NTBugtraq, I put out a message today telling everyone that the link was *NOT* the "official" version of SP5 and that they should avoid it. Downloading the version that was provided via the link would, at least, mean two copies of a 32MB file needed to be downloaded, and at worst, could cause serious problems due to its lack of completeness.

At the time of writing, however, Microsoft had made no "official" announcements...nor should they. They have *NOT* made an "official" announcement of it being available, so why make an announcement that says as much.

Whether people chose to listen to my NTBugtraq "official" message on the subject or not is a matter of trust, but its no more "official" than those saying SP5 RTM is available, is it.

FYI, whenever Microsoft makes a large download available from the 'net, backbones tend to suffer due to the huge volume of downloads that ensues. False messages about the availability of something like SP5 could lead to spikes in traffic unnecessarily, and other sundry problems. At least, it compounds the issues surrounding web distribution of large files.

Russ - NTBugtraq moderator

Outdated address books

"Robert David Graham" <rob@netice.com>

Sat, 1 May 1999 20:21:22 -0700

When registering the domain for the startup I work for, I apparently re-registered an old domain that somebody else let lapse. As a result, I occasionally get mail destined for people in that old domain.

The majority of such e-mail are actual correspondences because people haven't updated their address books. To illustrate the RISK, consider the following e-mail I received:

```
> Xxxxx,  
>  
> I'll be away now for 8 weeks and will be having my mail  
intercepted by  
> our receptionist who is the kind of person who would have me  
sacked for  
> the type of mail that I've been receiving lately, so could you  
please  
> not send me any messages until I return.  
>  
> Also, when mail is sent to a list of people including myself,  
the mail  
> comes into our server as an inbound message failure, and then  
gets read  
> by the receptionist before forwarding. Unfortunately this is  
what  
> happened to the previous message 'ouch!' - hopefully the  
attachment  
> wasn't opened.  
>  
> cheers,  
> Yyyyy
```

I enjoy contemplating the forged e-mails I could send him (which will get intercepted by the secretary). Any ideas?

Robert Graham, CTO, Network ICE

✦ Israeli scientist reports discovery of advance in code breaking

Edupage Editors <edupage@franklin.oit.unc.edu>

Mon, 3 May 1999 11:56:16 -0600

Israeli computer scientist Adi Shamir is expected to present a paper outlining the design of a yet-to-be-built-machine that could quickly decipher computer generated codes. Shamir -- who represents the 'S' in RSA encryption design -- will present his paper this week at the International Association for Cryptographic Research in Prague, which begins Monday. Shamir's idea would combine existing technology into a special task computer that would make factoring numbers as long as 150 digits much easier. As a result, codes accepted as reasonably secure for financial transactions and government communications would be much easier to decipher. Researchers say the machine could be built at a relatively low cost, and that key systems of 512 bits or less (keys of about 140 digits or less) would be vulnerable. Longer 1,024-bit keys would still be out of reach for Shamir's new machine. (*The New York Times*, 2 May 1999; Edupage, 3 May 1999)

✦ Re: CIH virus

"Matthew Todd" <matthew@mail.cmb.ac.lk>

Mon, 3 May 1999 13:49:37 +0600

The [Colombo] Sunday Times

<http://www.lacnet.org/suntimes/990502/spec.html>

<http://www.lacnet.org/suntimes/990502/plusm.html#label0>

<http://www.lacnet.org/suntimes/990502/plusm.html#1LABEL1>

<http://www.lacnet.org/suntimes/990502/bus2.html#2LABEL2>

and Sunday Observer

<http://www.lanka.net/lakehouse/1999/05/02/fea33.html>

of 2 May 1999 both carry extensive coverage of the impact of the CIH virus, both in Sri Lanka and the rest of the world.

Some of those affected here include:

Yes FM, where one presenter reported the loss of five years' worth of data.

John Keells Computer Services, where IT Manager of Software Development

Services, Milinda Gunasena, was unaware of the virus and lost over 200 files

and spent all day cleaning the system.

DHL lost 15 computers, Forbes Tea Department three, and NIIT, an Information

Technology firm lost five machines.

The total damage here appears to be far less than in some other countries,

notably South Korea, but this has clearly been a very serious incident

throughout the region.

Although these articles also contain some technical inaccuracies common in

mass media coverage of events such as this, there are also some interesting

rumours/myths which are also originating: "At least four computer vendors

who did not wish to be identified said they suspected the virus originated from a particular company" meaning it had been released by an anti-virus software supplier...

Much of the coverage here has highlighted the fact that this virus seems to have done most of its damage in Asia, and that this is largely due to the extensive use of pirated software. This is largely due to inadequate legislation and enforcement -- currently in Sri Lanka, the law does not specifically protect copyright and intellectual property rights in computer software, and no doubt this is also true in much of the rest of Asia.

However, the problem is not only inadequate legislation. It is possible to buy a licensed and up to date version of a program here if you have sufficient money, however, the cost of much of the "standard" software which everybody wants is very high -- this is largely due to the huge profits which organisations like Microsoft chooses to make -- and the fact that many hardware vendors install software (illegally?) at the point of sale, means that many users have no idea of the origin or provenance of the software they use.

Much has also been made in the press here of the lateness of the warnings put out by the national IT bodies such as CINTEC. The possibility is even hinted at, and no doubt will meet with some public approval, that the lateness of the warnings makes anyone who knew about the virus in advance responsible.

Results (apart from the damage done):

- sales of anti-virus software have soared. Presumably these are all original disc rather than pirated, and will come with the appropriate periodic upgrades.
- CINTEC (national IT council) is to establish some form of early warning section to keep the user community better informed.

Outstanding issues (inter alia)(many no doubt familiar to RISKS readers):

- Giving appropriate warnings in time -- the danger of "crying wolf" needs to be borne in mind. Also the risk of media caused panic should be borne in mind by any group set up by CINTEC.
- Establishing appropriate legislation and enforcement regarding software piracy.
- Better education of IT users, not just to purchase anti-virus products, but to introduce procedures for ensuring they are used and kept up to date.

⚡ Re: MS-Outlook 98 risk of mislaying messages in Outlook today

GRANT Jedediah <jgrant@namsa.nato.int>

Mon, 3 May 1999 07:18:25 +0100

I've also encountered subject item noted in RISKS. However, it is possible using the Advanced Find for a user to see the messages dropped on

Outlook Today. A simple advanced find with no parameters other than to look for all messages in the users mailbox will reveal the hidden items in Outlook Today as located in the "Top of Information Store" folder.

J. Grant (jgrant@namsa.nato.int)

Smart Card Forum Privacy Symposium, 20 May 1999

"Donna Farmer" <dfarmer@smartcardforum.org>

Mon, 3 May 1999 14:16:30 -0400

'Enabling Privacy in a Virtual World' 20 May 1999

See <http://www.smartcardforum.org> or by call (202) 530-5306.

For information about The Smart Card Forum:

Patrick Corman, Corman Communications, (650) 326-9648

patrick@cormancom.com

Nancy MacGregor <nancy@cormancom.com> (415) 643-0766



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 38

Friday 7 May 1999

Contents

- [Sixth satellite launch failure in less than nine months](#)
[PGN](#)
- [Israeli scientist reports discovery of advance in code breaking](#)
[Bruce Schneier](#)
- [Bernstein Decision Upheld](#)
[Lauren Gelman](#)
- [Export controls lose appeal](#)
[Adam Shostack](#)
- [Computer glitches foul up flights at Chicago airports](#)
[Keith A Rhodes](#)
- [Star Wars tchatchkis bring down eBay server](#)
[PGN](#)
- [Oops! Intel "accidentally" sues potential partner](#)
[Lenny Foner](#)
- [New Coke machine goes wireless and cashless](#)
[Mark Gregory](#)
- [New area code creates accidental phone forwarding risk](#)
[Philip Koopman](#)
- [Re: Bloatware Debate](#)
[Dick Mills](#)

- [E-mail address not optional?](#)
[David Keegan](#)
 - [Security/privacy hole in Chase Online Banking](#)
[Daniel Norton](#)
 - ["The Vortex Daily Reality Report and Unreality Trivia Quiz"](#)
[Lauren Weinstein](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Sixth satellite launch failure in less than nine months

"PGN" <Neumann@csl.sri.com>
Fri, 07 May 1999 11:56:17 -0500

On 4 May 1999, a Boeing Delta III rocket launch dumped Loral's Orion communications satellite in an orbit from 98 to 862 miles. A previous launch try two weeks before had gone to the countdown of zero, but a software flaw prevented ignition. The first Delta III launch ended after 71 seconds when the rocket exploded because of a software flaw that caused the hydraulic fuel to be expended prematurely. [*The Washington Post*, 6 May 1999, PGN-ed]

So, we have had three military satellites stuck in useless orbits, two aerospace launch explosions, and a private satellite that seems to have disappeared (Ikonos 1), \$3.5M expended. Boeing and Lockheed Martin have both been victimized. The Shuttle Columbia is grounded, pending study of the Titan IV failures. [From AP items, 6 May 1999, PGN-ed]

⚡ Israeli scientist reports discovery of advance in code breaking

Bruce Schneier <schneier@counterpane.com>

Wed, 05 May 1999 15:10:40 -0500

Factoring with TWINKLE

At Eurocrypt '99, Adi Shamir presented a new machine that could increase our factoring speed by about 100-1000 times. Called TWINKLE (The Weizmann INstitute Key Locating Engine), this device brings 512-bit keys within the realm of our ability to factor.

The best factoring algorithms known to date all work on similar principles.

First, there is a massive parallel search for equations with a certain relation. This is known as the sieving step. Then, after a certain number of relations are found, there is a massive matrix operation to solve a linear equation and produce the prime factors. The first step can easily be paralleled--recently, 200 computers worked in parallel for about four weeks to find relations to help factor RSA-140--but the second has to be done on a single supercomputer: it took a large Cray about 100 hours and 810 Mbytes of memory to factor RSA-140.

Shamir conceptualized a special hardware device that uses electro-optical techniques to sieve at speeds much faster than normal computers. He encodes various LEDs with values corresponding prime numbers, and then uses it to factor numbers. The machine reminds me of the famous Difference Engine of the 1800s. Once the engineering kinks are worked out--

and there are considerable ones--this machine will be as powerful as 100-1000 PCs for about \$5000. The basic idea is not new; a mechanical-optical machine built by D.H. Lehmer in the 1930s did much the same thing (although quite a bit slower).

As far as we know, Shamir's machine is never been built. (I can't speak for secret organizations.) As I said, Shamir presented a conceptualization and a sketch of a design, not a full set of engineering blueprints. There are all sorts of details still to be figured out, but none of them seem impossible. If I were running a multi-billion dollar intelligence organization, I would turn my boffins loose at the problem.

The important thing to note is that this new machine does not affect the matrix step at all. And this step explodes in complexity for large factoring problems; its complexity grows much faster than the complexity of the sieving step. And it's not just the time, it's the memory requirements. With a 1024-bit number, for example, the matrix step requires something like ten terabytes of memory: not off-line storage, but real computer memory. No one has a clue how to solve that kind of problem.

This technique works just as well for discrete-logarithm public-key algorithms (Diffie-Hellman, ElGamal, DSA, etc.) as it does for RSA. (Although it is worth noting that the matrix problem is harder for discrete-log problems than it is for factoring.) The technique does not

apply to elliptic-curve-based algorithms, as we don't know how to use the sieving-based algorithms to solve elliptic-curve problems.

In Applied Cryptography, I talked about advances in factoring coming from four different directions. One, faster computers. Two, better networking. Three, optimizations and tweaks of existing factoring algorithms. And four, fundamental advances in the science of factoring. TWINKLE falls in one and three; there is no new mathematics in this machine, it's just a much faster way of doing existing mathematics.

Shamir's contribution is obvious once you understand it (the hallmark of a brilliant contribution, in my opinion), and definitely changes the landscape of what public-key key sizes are considered secure. The moral is that it is prudent to be conservative--all well-designed security products have gone beyond 512-bit moduli years ago--and that advances in cryptography can come from the strangest places.

Shamir's paper:

<http://jya.com/twinkle.eps>

Bruce Schneier, President, Counterpane Systems Phone: 612-823-1098
101 E Minnehaha Parkway, Minneapolis, MN 55419 <http://www.counterpane.com>

Bernstein Decision Upheld

Lauren Gelman <gelman@turing.acm.org>

Thu, 6 May 1999 19:03:33 -0400

Today, the 9th Circuit Court of Appeals upheld the district court's findings that the provisions of the Export Administration Regulations ("EAR") that limit Bernstein's ability to distribute encryption software constitute a prior restraint on speech under the First Amendment.

In the Courts analysis they found source code to be expressive speech demanding the highest First Amendment protection. Therefore, they determined that EAR operated as a prior restraint that burdens scientific expression. Because the prepublication licensing scheme grants a great amount of discretion to public officials and fails to contain adequate procedural safeguards against selective enforcement, the gvt failed to meet the heavy burden required for regulating expressive speech.

In its conclusion, the court also stated that "the government's efforts to retard progress in cryptography may implicate the Fourth Amendment, as well as the right to speak anonymously." However this text is not binding (It is "dicta" not related to the challenge Bernstein asserted).

I have included some excerpts from the decision below. The full text of the decision can be found at:
http://www.epic.org/crypto/export_controls/bernstein_decision_9_cir.html

The amicus brief USACM signed can be found at:
http://www.epic.org/crypto/export_controls/bernstein_brief.html

-Lauren

Excerpts:

[2] The Supreme Court has treated licensing schemes that act as prior restraints on speech with suspicion because such restraints run the twin risks of encouraging self-censorship and concealing illegitimate abuses of censorial power. See *Lakewood v. Plain Dealer Publishing Co.*, 486 U.S. 750, 759 (1988). As a result, "even if the government may constitutionally impose content-neutral prohibitions on a particular manner of speech, it may not condition that speech on obtaining a license or permit from a government official in that official's boundless discretion."

[4] The EAR regulations at issue plainly satisfy the first requirement -- "the determination of who may speak and who may not is left to the unbridled discretion of a government official." *Id.* at 763. BXA administrators are empowered to deny licenses whenever export might be inconsistent with "U.S. national security and foreign policy interests." 15 C.F.R. S 742.15(b). No more specific guidance is provided. Obviously, this constraint on official discretion is little better than no constraint at all. See *Lakewood*, 486 U.S. at 769-70 (a standard requiring that license denial be in the "public interest" is an "illusory" standard that "renders the guarantee against censorship little more than a high-sounding ideal."). The government's assurances that BXA administrators will not, in fact, discriminate on the basis of content are beside the point.

As noted earlier, the chief task for cryptographers is the development of

secure methods of encryption. While the articulation of such a system in layman's English or in general mathematical terms may be useful, the devil is, at least for cryptographers, often in the algorithmic details. By utilizing source code, a cryptographer can express algorithmic ideas with precision and methodological rigor that is otherwise difficult to achieve. This has the added benefit of facilitating peer review -- by compiling the source code, a cryptographer can create a working model subject to rigorous security tests. The need for precisely articulated hypotheses and formal empirical testing, of course, is not unique to the science of cryptography; it appears, however, that in this field, source code is the preferred means to these ends.

[5] Thus, cryptographers use source code to express their scientific ideas in much the same way that mathematicians use equations or economists use graphs. Of course, both mathematical equations and graphs are used in other fields for many purposes, not all of which are expressive. But mathematicians and economists have adopted these modes of expression in order to facilitate the precise and rigorous expression of complex scientific ideas.¹³ Similarly, the undisputed record here makes it clear that cryptographers utilize source code in the same fashion.¹⁴

[6] In light of these considerations, we conclude that encryption software, in its source code form and as employed by those in the field of cryptography, must be viewed as expressive for First Amendment purposes, and thus is entitled to the protections of the prior restraint doctrine. If the

government required that mathematicians obtain a prepublication license prior to publishing material that included mathematical equations, we have no doubt that such a regime would be subject to scrutiny as a prior restraint. The availability of alternate means of expression, moreover, does not diminish the censorial power of such a restraint -- that Adam Smith wrote *Wealth of Nations* without resorting to equations or graphs surely would not justify governmental prepublication review of economics literature that contain these modes of expression.

We emphasize the narrowness of our First Amendment holding. We do not hold that all software is expressive. Much of it surely is not. Nor need we resolve whether the challenged regulations constitute content-based restrictions, subject to the strictest constitutional scrutiny, or whether they are, instead, content-neutral restrictions meriting less exacting scrutiny. We hold merely that because the prepublication licensing regime challenged here applies directly to scientific expression, vests boundless discretion in government officials, and lacks adequate procedural safeguards, it constitutes an impermissible prior restraint on speech.

Second, we note that the government's efforts to regulate and control the spread of knowledge relating to encryption may implicate more than the First Amendment rights of cryptographers. In this increasingly electronic age, we are all required in our everyday lives to rely on modern technology to communicate with one another. This reliance on electronic

communication,
however, has brought with it a dramatic diminution in our
ability to
communicate privately. Cellular phones are subject to
monitoring, e-mail is
easily intercepted, and transactions over the internet are often
less than
secure. Something as commonplace as furnishing our credit card
number,
social security number, or bank account number puts each of us at
risk. Moreover, when we employ electronic methods of
communication, we often
leave electronic "fingerprints" behind, fingerprints that can be
traced back
to us. Whether we are surveilled by our government, by
criminals, or by our
neighbors, it is fair to say that never has our ability to
shield our
affairs from prying eyes been at such a low ebb. The
availability and use of
secure encryption may offer an opportunity to reclaim some
portion of the
privacy we have lost. Government efforts to control encryption
thus may well
implicate not only the First Amendment rights of cryptographers
intent on
pushing the boundaries of their science, but also the
constitutional rights
of each of us as potential recipients of encryption's bounty.
Viewed from
this perspective, the government's efforts to retard progress in
cryptography may implicate the Fourth Amendment, as well as the
right to
speak anonymously, see *McIntyre v. Ohio Elections Comm'n*, 115 S.
Ct. 1511,
1524 (1995) , the right against compelled speech, see *Wooley v.*
Maynard, 430
U.S. 705, 714 (1977), and the right to informational privacy,
see *Whalen v.*
Roe, 429 U.S. 589, 599-600 (1977). While we leave for another
day the
resolution of these difficult issues, it is important to point
out that

Bernstein's is a suit not merely concerning a small group of scientists laboring in an esoteric field, but also touches on the public interest broadly defined.

Association for Computing, + <http://www.acm.org/usacm/>
Office of U.S. Public Policy * +1 202 544 4859 (tel)
666 Pennsylvania Ave., SE Suite 302 B * +1 202 547 5482 (fax)
Washington, DC 20003 USA + gelman@acm.org

✦ Export controls lose appeal

Adam Shostack <adam@homeport.org>
Fri, 7 May 1999 09:45:09 -0400

In Bernstein v. USDOJ:

<http://www.ce9.uscourts.gov/web/newopinions.nsf/f606ac175e010d64882566eb00658118/febd2452a8a4d79b8825676900685b71?OpenDocument>

"Because the prepublication licensing regime challenged by Bernstein applies directly to scientific expression, vests boundless discretion in government officials, and lacks adequate procedural safeguards, we hold that it constitutes an impermissible prior restraint on speech. We decline the invitation to line edit the regulations in an attempt to rescue them from constitutional infirmity, and thus endorse the declaratory relief granted by the district court."

✶ Computer glitches foul up flights at Chicago airports

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

Fri, 07 May 1999 11:30:19 -0500

The Chicago area TRACON in Elgin was testing new software on 5 May 1999 that displays aircraft sizewise. As a result of problems, there were serious traffic problems at O'Hare and Midway. Even after fixes were made, delays continued. United cancelled 25% of its afternoon flights, American 13%.

[Source: Associated Press, 5 May 1999; PGN-ed]

[Note: Why worry about Y2K when the day-to-day problems keep you busy enough? By the way, these contingency plans will not work in a Y2K

environment if the FAA experiences simultaneous multiple system failures.

In this case, they never lost sight of the planes and were always in voice

contact. That's fine, so long as you have voice communications and a way to track the aircraft. KAR]

✶ Star Wars tchatchkis bring down eBay server

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

Tue, 4 May 99 14:52:47 PDT

Beginning soon after the Star Wars goodies went on sale in stores at 12:01a.m. on 3 May 1999 EDT, and most noticeably around 2:30am EDT, eBay auctions ceased when a server saturated. In contrast, Amazon was going full blast by noon PDT, auctioning off toys and other items related

to the
long-awaited Star Wars: Episode I -- The Phantom Menace.

When it comes to Star Wars (the movie) computer support or
StarWars (the
defense system),

May the flaws be with you.

Oops! Intel "accidentally" sues potential partner

Lenny Foner <foner@media.mit.edu>

Wed, 5 May 1999 17:04:22 -0400

I can see it now -- World War III will start, not with an
accidental
launch, but with an accidental lawsuit...

Last week, the Taiwanese chipmaker Via Technologies received a
package in
the mail containing court documents from Intel, a potential
business partner
with whom they had been working on a cross-licensing agreement.
It turned
out that Intel had written a draft contingency lawsuit and had
accidentally
filed it in US District Court in San Jose. By law it could not
be
withdrawn, but Intel filed for dismissal the same day.

[Source: Intel: To Sue Is Human, by Leander Kahney, 4 May 1999,
PGN-ed;

http://www.wired.com/news/print_version/business/story/19486.html?wnpg=all]

[Really tells ya how they think, eh? While one hand is
offering to do
business, the other is preparing to sue... Lenny]

⚡ New Coke machine goes wireless and cashless

"Mark Gregory" <oreo@eudoramail.com>

Wed, 05 May 1999 06:52:07 -0700

"The Coca-Cola Company is testing a new vending machine that lets thirsty consumers pay for a Coke on credit by dialing a special phone number located on the machine near the coin slot. When consumers dial the number, their selection pops out and their wireless phone account is charged for the beverage. Students and staff at the Institute of Technology in FINLAND are using the prototype. "

Now, if I want a Coke, could I page someone with a cell phone to the special phone number?

⚡ New area code creates accidental phone forwarding risk

Philip Koopman <koopman@cmu.edu>

Mon, 03 May 1999 23:49:54 GMT

This was posted by our CS facilities manager today:

> Some folks in SCS have been suddenly finding their phones forwarded
>to off-campus locations, especially if their homes are in the new 724 area
>code. The cause and cure are simple. On CMU's Centrex phone system,
>one dials "172" to forward a line to another location. What seems to be
>happening is that, when dialing numbers in the new area code,

some folks

>inadvertently forget to dial a "9" before dialing "1" and the 10-digit number.

>When this happens, Centrex sees the string "172" followed by what may

>be a valid seven-digit number. So phones get forwarded to weird places

>and the user isn't aware of it until someone tells them. If this happens

>to you, the fix is simple: pick up the phone receiver and dial "173",

>which is Centrex's cancellation code for call forwarding.

And, in a separate incident, I was in an office visiting someone whose

new telephone number catches one or two wrong number calls per hour. It

seems that their extension number starts with the three digits of the

local phone exchange, so a fraction of people dialing off-premises get

that number by mistake if they forget to dial the leading "9".

I suppose both these stories re-emphasize the known RISK of failing to

provide safety nets for people who forget to dial access prefixes.

Phil Koopman -- koopman@cmu.edu -- <http://www.ece.cmu.edu/~koopman>

[The second one is a characteristic problem, and has been in RISKS in several forms over the years. PGN]

⚡ Re: Bloatware Debate (Downes, [RISKS-20.35-37](#))

Dick Mills <dmills@albany.net>

Tue, 04 May 1999 18:02:42 -0400

Many thanks to RA Downes for a well documented illustration of bloat.

At Jonathan Goldberg and others point out, it is considered beneath the dignity of software professionals to concern themselves with such minutia. Hardware is inexpensive.

I remember similar discussions in the 1970s about bloat in compiled programs compared to assembler. Eventually compiler optimization became so good that the best programmers couldn't beat the compilers in making the code efficient.

It took very many years afterward to convince programmers to write clear code and let the compiler worry about making it efficient. It sounds like we may have fooled ourselves. While concentrating on compiler optimizations at the front door, some of us didn't notice bloat coming in via the non-language-related back door.

If Mr. Downes can identify the bloat and determine that it is not needed, then software can do it too. Bloat elimination could be automated. The software to do it could come from Microsoft, or from third parties. It could work within the development environment or it could work with EXE and DLL files.

That sounds like an opportunity for some smart person to make money. Any takers?

Dick Mills

<http://www.albany.net/~dmills>

⚡ E-mail address not optional?

David Keegan <dksw@tinet.ie>

Thu, 6 May 1999 11:38:38 +0100

I contracted in-house at an organization with about 1000 staff recently, and was given an e-mail address when I started work. After several months I began to receive e-mail messages which were obviously not intended for me.

Apparently another David Keegan had joined the company, but had not yet been given an e-mail address. However, people (and programs) trying to contact him could all too easily input "David Keegan" into the e-mail client's address book, get my address in response, and assume it was the right one.

The misdirected messages continued for several weeks. Mostly they were of no consequence. However there were several marked "Confidential", and some of these contained passwords and other sensitive information. It amounted to a serious breach of security in an organization which was normally very security conscious.

I eventually contacted my namesake (with some difficulty, since I couldn't use e-mail!) and persuaded him that he should get an e-mail address. This reduced the number of misdirected messages, but did not eliminate them completely. Now the e-mail client popped up a list of two e-mail addresses for "David Keegan", but there wasn't enough information displayed to ensure

that the user always picked the right one.

My conclusion is that in a company using e-mail, an employee without an address is a potential security risk.

David Keegan

[DK Software Ltd Engineers and Consultants dksw@tinet.ie]
[56 Roebuck Downs Dublin 14 IRELAND]

✶ Security/privacy hole in Chase Online Banking

Daniel Norton <Daniel@DanielNorton.net>

Thu, 06 May 1999 12:40:08 GMT

Here's an excerpt from a letter I faxed to Chase Online Banking (www.chase.com) the other day. Not only have they not fixed the problem, they apparently didn't consider it a big enough risk to reply to my letter.

It was particularly difficult to find someone at chase who knew what I was talking about (I'm not convinced I ever did):

=====

CHASE ONLINE BANKING
Attn: Yvonne Woods
Attn: Daryl Stimley

Dear Sir and Madam,

I am writing to report a serious security problem with your Chase Online Banking web service. The problem is best described by example:

- 1) A customer signs onto the service, giving an account and password.
- 2) The accesses information on the service.

- 3) The customer signs off.
- 4) The system reports that the session has exited.
- 5) A different person can now fully access the account.

It has been difficult to get in touch with the right person that understands this. I was referred to Abdul Gbabamosi, but he clearly has no understanding of the problem at all and he point-blank denied that I actually saw the above scenario occur.

You can review a test I just made. It shows I signed on today at "6:03 pm ET" and signed off at "6:07 pm ET". I then accessed my account without entering my account number and password and signed off again. The log should show that I signed off again at "6:09 pm ET". The COB account number for my business is [deleted-DAN].

This problem raises the greatest risk for people who access the service from public terminals, but can also pose a problem even for people who access the service at home who might not want other family members having full access to the account.

I hope you are more effective at addressing the problem than you are at allowing me to report it.

Sincerely,

/ss Daniel A. Norton/
President

 **"The Vortex Daily Reality Report and Unreality Trivia Quiz"**

Lauren Weinstein <lauren@vortex.com>

Wed, 05 May 99 19:05:31 PDT

Greetings. As the moderator of the PRIVACY Forum, I get a lot of e-mail, tending to run the gamut in a variety of ways... One frequent class of received messages is requests for comments or advice on matters concerning not only privacy but also a variety of related (and sometimes unrelated) fields, including many topics relating to RISKS. Since there tends to be considerable overlap between many such requests, suggesting common points of interest, I've now launched the audio program with the long name:

"The Vortex Daily Reality Report and Unreality Trivia Quiz"

It's available via RealAudio over the net, and is updated each day from Monday through Friday. Essentially, it's a daily brief blast of (my) opinionated commentary, focusing on exposing the fallacies of muddy thinking, crazy ideas, misguided concepts, and other related areas that seem to be sending the signal/noise ratio of our society down the drain. As you can imagine, privacy issues are included, but are but one of the topic areas covered. These short (just a minute or two) audio reports tend to be more opinionated than my National Public Radio commentaries, and cover a much wider range of subjects.

Each of these short audio reports also includes an "Unreality Trivia Quiz" question (and the answer to the previous program's question). What's an "unreality" question? Try it and see...

These daily features can be heard via a link at the main PRIVACY Forum page:

<http://www.vortex.com/privacy>

or can be played directly via the RealAudio file URL:

<http://www.vortex.com/reality.ram>

Please feel free to forward this announcement, or link to the associated program URLs, as you feel appropriate.

Comments, opinions, and ideas for segments are always welcome, of course!

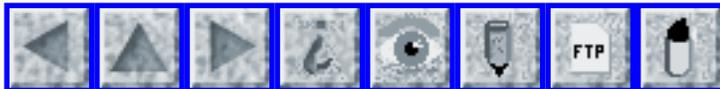
Thanks very much.

--Lauren--

Lauren Weinstein

Moderator, PRIVACY Forum

<http://www.vortex.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 20: Issue 39

Friday 14 May 1999

Contents

- [Hacker competition opens in Singapore with \\$10,000 prize](#)
[Keith A Rhodes](#)
- [Faulty software doomed Titan 4B Milstar launch](#)
[Keith A Rhodes](#)
- [MI6 Agents 'outed' by Web](#)
[Randy Holcomb](#)
- [41-year-old died while NYC's 911 system was down](#)
[Monty Solomon](#)
- [``Human error'' posts budget PR on the web prematurely](#)
[George Michaelson](#)
- [Computer woes set back opening for Tulsa's jail](#)
[Jo Oerhlein](#)
- [C compilers vs editors: WYSI NOT ALWAYS WYG](#)
[Daniel A. Graifer](#)
- [Risks of upgrading a UNIX system](#)
[Wolfgang Moeller](#)
- [Any Bell Atlantic customer can be spuriously Opted Out from CALL54](#)
[Douglas A. Brothers](#)
- [SurfWatch filters out plugandpray.com and minow.org](#)
[Martin Minow](#)

- [MS AutoRoute Express 2000](#)
[Pete Mellor](#)
 - [Another talking lift bug](#)
[George Michaelson](#)
 - [On-line account access](#)
[Leo Sokolskiy](#)
 - [Wrong e-mail address](#)
[Bruce Wampler](#)
 - [Risks of 3-letter user IDs for free e-mail accounts](#)
[Dan Yurman](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Hacker competition opens in Singapore with \$10,000 prize**

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

Fri, 14 May 1999 10:07:33 -0500

Prizes up to \$10K are being offered to anyone who first penetrates supposedly secure Web servers at an information technology trade show in Singapore. The two servers are products of Voltaire Advanced Data Security in Israel [210.24.153.70] and Conclave Integrated Internet Security in California [210.24.153.90]. There is also a third (unprotected) server [210.25.153.80]. Successful penetrators must alert the organizers at hackerszoneAyahoo.com within one day of the hack. Conclave regional director George Kane said it had "100 percent confidence" that its server was hacker-proof. You must "break into two workstations, then the secure server, retrieve and change specified files, and then manage to leak the information into a public work station."

Voltaire's key security product is a device that physically divides one single personal computer into two workstations, guaranteeing separation of secured and unsecured environments.

Conclave utilizes an integrated system that includes a firewall, anti-virus and encrypting capabilities.

[Source: Agence France-Press item from Singapore, 13 May 1999]

✂ Faulty software doomed Titan 4B Milstar launch ([RISKS-20.36](#))

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

Thu, 13 May 1999 14:35:24 -0500

The 30 Apr 1999 improper Milstar orbit was the result of Lockheed Martin engineers loading flawed software into the Titan/Centaur rocket. The flaw was not detected despite extensive prelaunch "verification". The report will be published next week in *Aviation Week and Space Technology*. "The software was verified at Lockheed Martin Astronautics in Littleton, Colo. The work force there already had been stung by 900 impending job cuts and the murder of 12 students and a teacher at nearby Columbine High School." [Source: Article by Todd Halvorson, Florida Today, 8 May 1999, <http://www.flatoday.com/space/explore/stories/1999/050899b.htm>; PGN-ed]

⚡ MI6 Agents 'outed' by Web

"Holcomb, Randy" <RandyHolcomb@firstusa.com>

Thu, 13 May 1999 11:04:57 -0400

A 'disgruntled employee' has reportedly exposed the identities of over 100 MI6 agents on a Web site. [The U.K. government has insisted that the Web pages be removed, although apparently mirrors are popping up in other places. PGN-ed]

⚡ 41-year-old died while NYC's 911 system was down

Monty Solomon <monty@roscom.com>

Tue, 2 Feb 1999 12:07:14 -0500

Susan Ungvary repeatedly called 911 when her boyfriend collapsed, but repeatedly got busy signals. It turns out that the 911 system was down for over an hour, as a result of a routine test (four times each year since 1996) of emergency generators in which the backup system failed to forward calls to police headquarters. Whether the death could be attributed to the system outage is unresolved. [Source: Associated Press item, *The Boston Globe*, 2 Feb 1999, page A10; PGN-ed.

"http://www.boston.com/dailyglobe2/033/nation/As_41_year_old_died_NYC_s_911_was_busy+.shtml"

⚡ ``Human error'' posts budget PR on the web prematurely

George Michaelson <ggm@dstc.edu.au>
Wed, 12 May 1999 15:56:57 +1000 (EST)

I liked:

"result of a series of technical and human errors associated with preparations to meet the requirement for Budget information on government Websites immediately after the Budget speech"

Down here, and in the UK, it is routine for the Journalists to be in a lock-in with government flaks 2-3 hours ahead of the budget so they can do live comment based on advance knowledge. I bet somebody took the logical steps to make the Internet 'just as good as the lock-in'.

[<http://www.abc.net.au/news/newslink/nat/newsnat-12may1999-47.htm>]

⚡ Computer woes set back opening for Tulsa's jail

Jo Oerhleim <COehrlein@aol.com>
Fri, 14 May 1999 09:20:34 EDT

The new Tulsa County jail will be dedicated tomorrow, but it is not ready for prisoners -- because of software problems. A pervasive information system is supposed to track up to 1440 prisoners using bar-coded wristbands. EPIC Solutions (San Diego) implemented the system, but is finding the challenge more difficult than expected. [Source: Article by Larry Levy, *The Daily Oklahoman*, 14 May 1999, page 5]

⚡ C compilers vs editors: WYSI NOT ALWAYS WYG

"Daniel A. Graifer" <dgraifer@cais.com>

Fri, 14 May 1999 10:48:44 -0400

I recently sent some C source developed on unix to a colleague for modification and compilation under MS Windows. The resulting executable behaved in unexpected ways precisely at the points he modified. I have finally figured what happened.

The MS Visual Studio V5.0 he is using has a built in source editor that recognizes both Windows <CR><LF> and unix <LF> as "newline". The integrated C/C++ compiler will accept C++ style "//" comments in C source. In making his modifications, the colleague used "//" comments to suppress my code, then added new lines of his own code, sometimes above, sometimes below the suppressed entries. Apparently, the VC++ preprocessor or compiler didn't recognize the unix <LF> characters as termination of the commented out lines, and skipped everything up to his next entered line containing the required <CR><LF>!

This is the only situation in C/C++ I can think where it would matter.

Still, I think having the editor and the compiler from the same development platform have different definitions of "newline" is poor form. But just remember, What You See Is NOT What You Get!

Daniel A. Graifer <dgraifer@cais.com> Parker & Company 1-888-426-6548

Andrew Davidson & Company 588 Broadway, Ste 610, NY 10012 (212) 274-9075

⚡ Risks of upgrading a UNIX system

"GWDVMS::MOELLER" <moeller@gwdvms.dnet.gwdg.de>

Mon, 10 May 1999 22:26:19 +0200

When was the last time you rebuilt all privileged ('suid root') applications when upgrading a unix system, just in case?

I'm pretty sure one can find 'small print' that demands this, however I'm equally sure that hardly any system manager does so, since problems seem to occur very rarely. Here's a neat one:

Some time prior to the upgrade, system manager (S.M.) was asked to install 'sshd' on a not-so-common platform (nothing really security-relevant, machine used for raw speed only, users just being accustomed to that sort of login). Said platform (featuring a particularly elaborate user data base) requires some special calls (simple calling sequences) to be done during 'login' - no problem, 'sshd' knows about them, although not explicitly aware of the particular hardware. Cautiously, S.M. configures 'sshd' to not allow 'root' logins from the outside. What other harm could it possibly do?

Upgrade has to occur somewhat in a hurry, release documentation isn't on-site, but procedures are known well enough. S.M. asks the manufacturer's support representative if special precautions have to be taken, "errr, not that I'd think so". S.M. installs new version, all fine & dandy, even

remembers to check out `sshd' afterwards and finds it to work the same as before.

A couple of days later, S.M. logs in via `sshd' himself, and for the first time enters `su'. Gets very amazed at the new system's intelligence, as it knows to not ask him for a password. Minutes later, S.M. recognizes that `su' would never ask for a password, when the parent process had been created via `sshd' ... in spite of no other visible peculiarities with that process.

A re-build (pretty likely boiling down to nothing but a re-link) of `sshd' fixed the problem.

Quite a few years ago, when I saw the first mention of `ssh', I commented "If you're a bank, you don't buy your safe at a flea market; if you're not, you might be better off without a safe". Maybe there's some truth in it, after all.

Dr. Wolfgang J. "s."Moeller, Tel. +49 551 2011510, GWDG, D-37077 Goettingen, F.R.Germany <moeller@gwdvms.dnet.gwdg.de> <moeller@decus.decus.de>

P.S. re "software bloat":

Imagine uSoft going open source, and no-one going to have a look at it...

⚡ Any Bell Atlantic customer can be spuriously Opted Out from CALL54

<brothers@clark.net>

Tue, 11 May 1999 17:19:02 -0400 (EDT)

In the spring of 1999, Bell Atlantic-Virginia has notified its customers that it plans to introduce the Bell Atlantic CALL54(sm) service to its customers in northern Virginia. The CALL54 service is an automated reverse directory assistance service that will enable northern Virginia customers to obtain names and addresses for telephone numbers published by Bell Atlantic. Name and address information for telephone numbers in the entire states of Virginia and Maryland will be available at a charge of \$.75 per request of up to 3 numbers.

This service is already available in New Jersey, West Virginia and Maryland. Bell Atlantic will not provide name and address information for non-published numbers.

Customers with published telephone numbers may exclude their names and addresses from CALL54 service by calling toll free 1-877-678-6887 to "Opt Out" of the service. There is no charge to "Opt Out" of CALL54.

When you call their "Opt Out" service, you enter a ten-digit phone number and the system repeats it back to you. You are asked for a confirmation (depress 1) or cancellation (depress 2.).

What would prevent anyone in the world from opting you out of the service?

Would you be notified that you were "Opted Out?"

The process could be made considerably more secure by requiring that a subscriber call from the number being "Opted Out" or "Opted In"

and then
only giving the user the choice of "In" or "Out". There would be
no need to
enter a number as the phone company knows your number when you
call them.

Douglas A. Brothers <brothers@clark.net>

🔥 SurfWatch filters out plugandpray.com and minow.org

Martin Minow <minow@apple.com>

Fri, 7 May 1999 20:50:08 -0700

EXPLETIVE DELETED: SurfWatch, an Internet-filtering company that
aims to
protect children from online pornography and violence, boasts
that it only
blocks objectionable sites after "thoughtful analysis" by its
staff. This
left James Tyre, a Pasadena lawyer and Internet activist opposed
to
filtering, more than a little bemused when SurfWatch blocked his
newly
registered site, www.plugandpray.com for "sexually explicit
content." The
main problem: Mr. Tyre's site was and remains totally blank but
for an
innocuous banner ad. SurfWatch says its software most likely
confused
Mr. Tyre's site with a pornography site that shares the same
numerical
Internet protocol address in a setup called "virtual hosting."
SurfWatch
has since unblocked Mr. Tyre's site, but others haven't been so
lucky.
Martin Minow, a Silicon Valley programmer, recently discovered
that his new
site www.minow.org, was also blocked by SurfWatch for alleged
explicit
content. The site bears only the words, "This site is under

construction."

Theresa Marcroft, director of marketing for SurfWatch, concedes that the company's software tends to block even innocuous virtually hosted sites if they are added to an Internet address that has been previously blocked, although she notes that the company responds quickly to unblock clean sites once it knows about them. "We're doing our best," she says. "This is such a nit in the overall objective of keeping kids away from the objectionable stuff." [Compiled by Nicole Harris and Ann Grimes, Posted by James S. Tyre <j.s.tyre@cyberpass.net>, from *The Wall Street Journal*, 6 May 1999, B4]

MS AutoRoute Express 2000

Pete Mellor <pm@csr.city.ac.uk>

Tue, 11 May 1999 12:25:21 +0100 (BST)

The following is taken from the BBC Watchdog web pages (www.bbc.co.uk/watchdog). I would like to thank Gordon Brown <gordon@jdc-etype.demon.co.uk> for passing it to one of my colleagues.

AutoRoute Express 2000 Weekend Watchdog 07.05.99

In February, Microsoft launched the new AutoRoute Express 2000 journey planner. By entering the details of any journey you want to make, it will show you the best roads to use and calculates how long the drive will take. It predicts possible hold ups and even recommends scenic spots on the way. Now Microsoft has admitted to Weekend Watchdog that

Autoroute's directions could cause drivers to make unnecessary detours that add miles to their trips.

Richard Emery, a logistical planner from Bracknell, advises companies on the best routes for moving their goods. It literally pays Richard to know the quickest way from A to B.

Using Autoroute Express 2000, Richard planned a trip from his home to a charity office in Llanelli in South Wales. He knew it was a long way but was not sure how long it would take. The software came up with what appeared to be a good set of clear directions, providing almost door to door road names, and said that the journey should take 2 hours and 36 minutes. Then Richard programmed in two 10 minute service station breaks. The journey suddenly changed from 169 to 185 miles, and the time taken increased by 1 hour and 3 minutes.

Richard demonstrated the problem to Weekend Watchdog with a real journey from Swindon to Reading.

Autoroute Express 2000 says it is a distance of 49.3 miles and, without a coffee break, should take 51 minutes along the M4. Richard then programmed in a 10 minute stop at Membury Services, almost half way between Swindon and Reading on the motorway. Autoroute changed a 30 second round trip into a 33 minute drive through the countryside. The software ignores the fact that most service areas are connected to the motorway, and works out a route via

junctions and A roads to the back of the service station.

Richard has discovered that this is the case with routes all over England. For example, London to Nottingham, 127 miles with two short coffee breaks according to AutoRoute, will take 3 hours and 15 minutes. That leaves 1 hour and 5 minutes to get coffee.

Microsoft says it's very sorry Richard Emery has experienced such problems with Autoroute Express 2000. It says that it is "committed to resolving these issues in the next version of the product". The company has set up an Autoroute Express 2000 Hotline on 0345 002000, which is open until 10pm on May 7th and between 9-5pm from then on.

<http://www.bbc.co.uk/watchdog/stories/autorout.shtml>

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

[Actually, the shortest distance between two points may involve the pub nearest where you started. If after a few pints you forget which way you were going, the trip can be much shorter. PGN]

⚡ Another talking lift bug

George Michaelson <ggm@dstc.edu.au>
Wed, 12 May 1999 16:00:44 +1000 (EST)

I've mentioned the lifts in our building with an off-by-one error on the

floor.

Now I've noticed that if you select a 'DOWN' lift button, but get into an 'UP' lift, albeit empty, and with no real 'UP' calls on it, although you get to select 'DOWN' as a destination, it still vocalizes "going up" as it moves.. downwards.

The sole reason for talking lifts seems to be to help blind people. You can imagine that in an emergency (not that you should use lifts then anyway) there would be some concern that a talking lift can confuse the rider even if the delivery point is correct.

I'm sure this is an example of an I.T. system grafted onto the core workings of the lift: the latter are going to be subject to some kind of safety proofs since the lift operations depend on them. The vocalizer is seen as 'ephemeral' and its bugs don't matter except...

-George

✶ On-line account access

"Leonid (Leo) Sokolskiy" <sokolski@hsc.usc.edu>

Tue, 11 May 1999 09:39:34 -0700

Recently the bank which issued one of my credit cards, First USA, started to offer on-line account access. I decided to give it a shot: it is a nice system, letting you see your charges, etc. Imagine my surprise one day when after I logging in I was looking at someone else's list of

charges although the system listed them under my account number. When I went to the statements section, I could pull up images of previous statements from someone else's account including name, address, account number, and list of charges.

Amazingly, calls and e-mail to customer service produced little response beside weak assurances to "investigate and fix it". Thus, despite bank's repeated statements that they concerned and respectful of their customer's privacy, it does not seem to trickle down to implementation level.

⚡ Wrong e-mail address

Bruce Wampler <bruce@objectcentral.com>
Fri, 07 May 1999 18:36:59 -0600

I just received a very big e-mail file filled with several Microsoft Word documents from a name I did not recognize. My first reaction was to worry about the Melissa virus, but closer examination of the To: revealed a wrong e-mail address. The e-mail was addressed to "xxx@realitycentral.com". The documents were obviously confidential real estate contracts, and the intended address must have been "xxx@realtycentral.com" -- no "i".

I own the URL "realitycentral.com" which is presently parked. All e-mail to the site is automatically forwarded to me. There are a lot of parked URLs

waiting for development that probably forward e-mail, or even dump it.

A couple of risks are obvious here. First, one needs to be very careful when sending confidential material that it goes to the right place, and really gets there. Second, it is possible to send e-mail to a site and have it delivered anyway, even though there is no one with the specific address at that site. This would usually cause a bounced message. Unless the sender is informed by the ultimate recipient of the e-mail (which I did), they will never know their mail went to the wrong place. Finally, there is the risk of having a URL similar to another busy site, not unlike having a phone number similar to a busy business number -- one may get a lot of wrong numbers.

The topic of sending e-mail to the wrong address has no doubt been discussed before, but I thought this instance demonstrated a couple of interesting twists.

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

⚡ Risks of 3-letter user IDs for free e-mail accounts

"Dan Yurman" <n43w112@hotmail.com>

Sun, 9 May 1999 10:17:20 -0600

The proliferation of free e-mail services available from a 'portal' sites raises the question of how to insure your user ID is unique

among millions
of other current and especially prior users of these services.
For
instance, a quick tour of the major portals indicate free e-mail
is available
from the following locations. This is necessarily a
representative sample
of sites chosen more or less for convenience, and not for any
commercial
purpose. Perhaps as many as 20 million people have or have had
free e-mail
accounts these or other sites.

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

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

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

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

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

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

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

For those of you who are considering signing up for a free
hotmail e-mail
account, or for any of the others, consider this lesson learned
from a
friend. Don't sign up for a user ID on Hotmail, or any other
free e-mail
service, using the three letters of your initials. There may be
someone out
there, in fact count on it, who also has those initials, and who
may have
had a Hotmail or other free e-mail account prior to yours.

Hotmail, like other free e-mail services, "recycles" user IDs.
This is not
unlike what the phone company does with your number after you
move. After a
suitable period of time, it reissues the number to a new
customer.
Otherwise, it would run out of numbers. I'm not picking on
Hotmail, just
arbitrarily using them in this example since they are one of the

largest of
the free e-mail services.

This challenge is that you may not like what the previous
"owner" of your
three letter user ID was interested in getting over the
Internet. For
instance, suppose the three letters of your initials are 'ABC'
yielding a
Hotmail account of abc(at)hotmail(dot)com. So, if your name is
'Anna Belle
Cornwall,' (a made up name for this posting with any resemblance
to a real
person strictly coincidental) it may be the prior user of that
account name
was Archie Bunker Cooper (same disclaimer). If "Archie" was
into less than
mainstream interests, or worse, and signed up for mailing lists
on his
favorite subjects, now innocent Anne Belle is going to get that
stuff
because she now owns the account abc(at)hotmail(dot)com.

Not only will she get all of 'Archie's' solicited mailing list
material, she
will also get every piece of spam still hunting for valid e-mail
addresses
known to be linked to his user ID and interests. If she's
lucky, all she'll
get are some get rich quick schemes, the occasional porno come
on, and
offers to buy stamp / coin collections or HO train sets. It
could be a lot
worse, especially if "Archie's" ex-wife, his creditors, or other
malcontents
think they are still talking to him over the Internet. Of
course, "Anna
Belle" could try answer them, but usually at this point
explanations will
not work, and like trying to teach the proverbial pig to sing,
only wastes
her time and annoys the pig. The replies also tell spammers
they have a

valid e-mail address.

There is nothing she is going to be able to do about all that spam, and the other stuff, except close the account and get a new one. This could be very inconvenient if she had already told her friends and family about her new three letter user ID.

There are several good strategies to avoid this problem.

* Put a number in your hotmail or other free e-mail user ID after the 1st letter, e.g a2bc(at)hotmail(dot)com, or in any position after the first letter, except the last. Hotmail, unlike some others, requires the first position to be a letter to avoid having their sites being the origin of spam.

This strategy eliminates many heritage users IDs based on three initials.

Even with 26 letters in the alphabet, there are still a finite number of combinations. The available three letter combinations go from AAA to ZZZ.

Since Hotmail has millions of users, your probability of encountering a match using just the three initials of your name, based on a prior or current user, is very high. However, assigning an arbitrary number within the three letter sequence eliminates "collisions" with all users IDs based solely on three initials.

* Use at least four letters, e.g. abcd(at)hotmail(dot)com, which will also eliminate a pretty good percentage of the like instances of inheriting three letter user IDs that have been recycled. This decreases the

odds of encountering a match, but still raises the possibilities of "collisions" with people who have shifted user ID naming strategies from using their three initials to using their first names.

If you use four letters and a number, after the 1st position, you have significantly increased the odds that no one else will have ever had this user ID before you. Now you have not only eliminated letter letter user IDs based on initials, but also almost all user IDs based on first names. The exception is if you put the number in the last position, e.g. if "Anna Belle" chooses 'anna5' etc.

* For a maximum strength strategy to avoid duplication with previous e-mail user ID owners try at least four letters plus mixing in say the first two or three numbers of your house street address, last few digits of your zip code, birthday date of your dog, cat, goldfish, etc., or any other numeric sequence that is meaningful. If "Anna's" zip code is 95472, she could choose a user ID of A9n5n4bc(at)hotmail(dot)com.

So if the mythical "Anne Belle" wants a no hassle user ID, that no one among the millions of past Hotmail users have held, one of these simple strategies should do the job for her. However, don't put these numbers at the end of the letter sequence. Mix them in the middle. It is common for other online services like AOL and Prodigy to put numbers at the end of user IDs to avoid duplications.

* Pick an entirely non-obvious combination, say the bar code for your favorite beer brand, your initials combined with the current temperature (your choice of indoor or outdoor readings), or, as in my case, a geographic reference. I choose the nearest USGS map corner, but you could look up the lot lines of your home or apartment and get carried away with surveying coordinates. :-)

The drawback is that these strategies fly in the face of personalizing your free e-mail account with something that others will remember easily. The whole point of the free e-mail accounts is that they are part of "mass customization" marketing strategies so the portal companies may not like this advice, or at least not very much. In fact this advice may fall in the same category as the story about the engineer who had to choose between a talking frog and a beautiful princess. However, it will work. I'm assuming you've already done some customization of your own with your home ISP, and that your use of a free e-mail account is to keep some communications out of your priority e-mail inbox, or for other business or personal reasons.

Enjoy the Internet. Surf safely.

I am not affiliated with hotmail except as an end user of the service.

Dan Yurman n43w112@hotmail.com Eagle Rock, Idaho



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 40

Tuesday 18 May 1999

Contents

- [Nuclear plant Y2K: High risk-readiness or high-risk readiness?](#)
[Mike Perry](#)
- [Biometric risks](#)
[Dan Wallach](#)
- [Singaporean ISP scans users' PCs](#)
[Andrew Brydon](#)
- [ATMs gobble up cash cards](#)
[John Colville](#)
- [Web browsers, URL collisions, and all that...](#)
[Zygo Blaxell](#)
- [False Viruses](#)
[Thomas Gilg](#)
- [HotMail is no Early Bird: happy99.exe](#)
[Malcolm Pack](#)
- [Virus cleaner corrupts e-mail database](#)
[Diomidis Spinellis](#)
- [MIME-Messages: quoted-printable chars in URLs](#)
[Christoph Conrad](#)
- [New-fangled petrol pumps](#)
[Ian Chard](#)

- [Re: C compilers vs editors: WYSI NOT ALWAYS WYG](#)
[Roy O. Wright](#)
 - [Re: Wrong e-mail address](#)
[Andrew J Klossner](#)
 - [Re: Risks of 3-letter user IDs](#)
[Thayne Forbes](#)
 - [Dimwitted naughty-word filtering lives...](#)
[Daniel Rutter](#)
 - [REVIEW: "Removing the Spam", Geoff Mulligan](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Nuclear plant Y2K: High risk-readiness or high-risk readiness?

"Perry, Mike" <mperry@europa.dg.com>

Mon, 17 May 1999 16:05:42 +0100

I read this last week on Silicon.com's news site (<http://www.silicon.com>):

A US nuclear plant has received a warning from the Nuclear Regulatory

Commission (NRC) after fears were raised over the Y2K readiness of an

emergency backup generator. Massachusetts Congressman, Edward Markey,

said the NRC has written to the Pilgrim nuclear plant expressing concern

that the generator will not be able to keep the facility safe in the event

of a Y2K blackout. The plant's owner said the problem will be solved by

adjusting the temperature limit for the generator.

Well, that's alright then, I don't suppose that the temperature limiter

serves any valid safety purpose, nor that running it outside the limits

prescribed by the manufacturers carries any RISKS....

Mike Perry Data General Ltd

Biometric risks

Dan Wallach <dwallach@cs.rice.edu>

Fri, 14 May 1999 14:51:51 -0500

Bank United of Texas has said they're about to introduce retina scanners to authenticate their customers to an ATM [1]. No more PINs. No more plastic cards. The article says they'll be using technology from Diebold, although no such technology is described on Diebold's Web page [2].

RISKS readers should be well aware that there are three different kinds of authentication (something you know, something you have, or something you are), and relying strictly on any one is a recipe for disaster. A

particular concern with purely biometric authentication systems is that there's no way to revoke your retina and get a new one. If somebody manages to make a copy, you're out of luck.

Says the article: "In response to questions about privacy concerns, Bank United said the iris pictures will not be distributed to anyone outside the bank."

Naturally, this is deeply unassuring. Even assuming we don't have bad guys going around cutting out people's eyes, and even assuming the ATM vendor is smart enough to verify the eye has a pulse (i.e., it's still

connected to
its owner's head), there isn't a whole lot preventing some other
vendor from
photographing your iris and using your biometric against you.

Also from the article: ``It has a very high cool factor,'' Coben
said. ``We
think of it as James Bond meets stocks and bonds.``

Hopefully, Bank United will have a golden eye for detail, and
will never say
never again to poor authentication. I wouldn't want my
optometrist, Dr. No,
to have a view to a killing in ATM crime.

Dan Wallach, Rice University

[1]http://dailynews.yahoo.com/headlines/ap/technology/story.html?s=v/ap/19990514/tc/atm_eye_scanners_5.html

[2]<http://www2.diebold.com/products/diebatms.html>

[This message is clearly not just for YOUR EYES ONLY, but
should
scare THE LIVING DAYLIGHTS out of others as well. However,
with
potential eye damage from miscalibrated units, remember that
YOU ONLY LIVE TWICE (pronounced "TWO-EYES"). With all this
Bonding
going on, there must be a SCAN-DOLL in there somewhere. PGN]

Singaporean ISP scans users' PCs

Andrew Brydon <andrew@isbjorn.demon.co.uk>

Sat, 15 May 1999 07:09:50 +0100

Daily Telegraph (UK) Thursday 13th May 1999 - Connected (IT
pullout) p.2

Singaporean Internet provider SingNet has apologised to its

subscribers

after scanning their PCs without their knowledge. SingNet asked the Singaporean Home Affairs Ministry to help check the computers of its 200,000 subscribers in the wake of the damage caused by the CIH virus. Unfortunately for SingNet an anti-hacking program being used by a customer picked up scanning, which was reported to the police. The scan was traced back to the government. The company says it did not look at any confidential files but did find that 900 subscribers have virus- infected computers.

Andrew Brydon, Systems & Software Safety Analyst

⚡ ATMs gobble up cash cards

John Colville <colville@socs.uts.edu.au>

Mon, 17 May 1999 09:16:37 +1000

From AAP via Sydney Morning Herald, Monday may 17, 1999, p4 with insertions by JC in [].

Many St George Bank [Australia's fifth largest bank] customers were left short at the weekend when automatic teller machines gobbled up their cash cards as the bank installed a new computer system.

The bank refused to say how many customers lost their cards. [The bank probably do not know how many cards were 'gobbled' yet because they were closed from their normal Saturday morning trading in preparation for the changeover.]

A spokesman said the problem occurred because of the expiry

dates on certain
cards. Canberra resident, Mr Steve Pye, who lost his card on
Saturday, said
there would be no replacements until Wednesday for "people like
me with no
money in my pocket . . . "I'm as mad as hell about it."

John Colville, University of Technology, Sydney
Broadway, NSW, Australia, 2007 colville@socs.uts.edu.au +61-2-
9514-1854

🔥 Web browsers, URL collisions, and all that...

Zygo Blaxell <uryse0d5@umail.furryterror.org>
16 May 1999 04:05:45 -0400

This happened to me the other month: an interesting interaction
between two
convenience features in web browsers and operating systems.

Where I work there is an internal server (let's call it 'qqq')
that
maintains some data used by the group I work in. The machine
generates test
data and serves dozens of report pages all hyperlinked together
and
accessible via a web client. Because it's on a corporate
intranet, all
desktop machines that can access the server happen to be
configured such
that they are able to use the short version of the server's
name, rather
than the long version of the name. So instead of typing "qqq.
example.com",
users can just type "qqq" and the client's OS configuration for
DNS lookups
will find the right host. This is a convenient, time-saving
feature.

On the public Internet, by contrast, there is a widespread convention for a web server owned by "The Example Corporation" to be named "www.example.com".

No doubt this convention was influenced by Netscape's decision to automatically expand bare hostnames typed into the "Location" field by

prepending "www." and appending ".com". So instead of typing "www.example.com", a user can just type "example". This is a convenient, time-saving feature.

Some months ago, the nameservers here at my employer were slightly amnesic, and kept forgetting the DNS entry for our server. So some mornings we would

type 'qqq' into the Location: field of Netscape, and we would get "server

does not have a DNS entry," because neither 'qqq' nor 'qqq.example.com' nor

'www.qqq.com' existed. Although Netscape only reports 'qqq' in the dialog,

it does report the other names it tries in the status bar. This is mostly harmless.

One day, somebody set up a web site under the name 'www.qqq.com'.

From then on, whenever my employer's DNS server forgot the IP address of

'qqq.example.com' but could find 'www.qqq.com', Netscape would decide that

when I typed 'qqq' I must have meant 'www.qqq.com', since neither 'qqq'

itself nor 'qqq.example.com' exist, and would proceed with its request using

the new host name.

To make matters worse, Netscape can sometimes do this even after it has

already done the DNS lookup on the host name. If this happens at just the

wrong time, it means that the remote system with the similar

name gets all
the information we would have sent to our own server: names and
passwords
used to authenticate with the local server, any cookies set by
programs on
the server, and usually a few user ID's and file names in the
URLs.

If our clients were point-of-sale terminals, this data could
have included
everything from credit card numbers and purchase details to
complete credit
histories from applications for financing.

Interestingly enough, this problem never happened at one of my
former
employers, which has a different policy for corporate host
names. They
insist on naming all hosts according to a company-wide encoding
system that
includes machine type, function, location, partial encoding of
the IP
address, and a check digit, which results in tens of thousands
of machines
with host names like "n3rndghh" or "amhjrxml". To date I know
of nobody who
has ever registered the domain name "www.n3rndghh.com", nor any
other .com
domain name that is valid in the scheme used by my former
employer, so there
have probably been no such collisions to date (although of
course it's
always possible to cultivate one).

Zygo Blaxell, Linux Engineer, Corel Corporation. zygod@corel.ca
(work) or
zblaxell@furryterror.org (play).

False Viruses

"GILG,THOMAS J (HP-Corvallis,ex1)" <Thomas_Gilg@ex.cv.hp.com>

Mon, 17 May 1999 15:08:59 -0700

When the Melissa virus hit, everyone in our R&D software lab updated their virus checkers and went into inoculation and quarantine mode. Several weeks later, I tried to run one of my old utility applications written in Microsoft Visual Basic (VB) and compiled into a .exe, and it was suddenly flagged as a "Backdoor.Trojan" virus. While the UNIX & Java in me saw great humor in it, I was no longer able to run a useful app.

Debugging the situation, I found that some function calls from a VB app into a Visual C++ COM object resulted in some VB .exe code that looked like a virus. Changing the type, order and number of parameters in a function call and/or changing the location from which the function call was made would influence whether or not the resulting .exe looked like a virus. For those interested, I spent most of my time reproducing the problem with:

```
.idl:    ... HRESULT test([in] BSTR foo, [in] int bar)
.h:     STDMETHODIMP(test)(/*[in]*/ BSTR foo, /*[in]*/ int
bar)
.cpp  STDMETHODIMP MyClass::test(BSTR foo, int bar)

.bas   mc.test "Hi", 2
```

I reported the problem to the virus checker company, and they confirmed some "false detection" cases. Fortunately for both of us, their latest virus definition update contained a fix for this problem. Unfortunately for some other folks in our lab, they ran into the same false virus alert with their VB apps and they removed them without question.

Clearly viruses and the code to detect them are getting extremely complex, so the opportunity for false alerts will do nothing but rise. It also occurred to me that the publication of false alert notices has its own set of risks.

Thomas Gilg, R&D Software Engineer, Hewlett-Packard
thomas_gilg@hp.com

✶ HotMail is no Early Bird: happy99.exe

Malcolm Pack <mpack@email.com>
Sat, 15 May 1999 08:57:59 +0100

A colleague at work was browsing his personal e-mail on HotMail, and asked me innocently if I knew what "HAPPY99.EXE" was, since someone he knows had sent it to him as an attachment. I explained that it was a "worm", and he should:

- o Delete it in situ, rather than download it.
- o Inform the sender of their infection.
- o Point them at a URL with suitable removal instructions[0].
- o Advise them to contact other people they might have e-mailed recently and warn them of the worm, etc.[1]

He also elected (belatedly) to run HotMail's live Virus Scan, ostensibly an implementation of NAI's McAfee, over the attachment.

It reported nothing amiss.

Note that locally-running versions of McAfee Virusscan will correctly identify the worm as W32/Ska.exe.

I have requested an explanation from HotMail, and will forward what I receive.

In the meantime, trust no one[2].

[0] Interestingly, an Infind <<http://www.infind.com>> search for sites referencing "HAPPY99" turned up one personal site which offered for download an executable to effect removal. I naturally chose to ignore this program of unknown provenance. Oh, how the risks mount up.

[1] So we have a whole series of legitimate e-mail warnings flying around in competition with the hoax e-mail warnings flying around and the warnings to ignore the hoax e-mail warnings flying around and...

[2] Especially if his initials are BG, and his company creates operating systems which are virus-friendly[3], but owns an on-line mail system which seemingly fails to spot those same viruses.

[3] And publically blames anti-virus software for a third of all crashes of its most "robust" OS.

Malcolm Pack <mpack@email.com>

⚡ Virus cleaner corrupts e-mail database

Diomidis Spinellis <dspin@aegean.gr>

Tue, 18 May 1999 11:39:59 +0200

I was told the following story by an associate who is managing a large distributed IT installation. The administrators at one site installed an anti-virus product on a machine running the Microsoft Exchange e-

mail server. Exchange keeps all incoming mailboxes in a monolithic database of a proprietary format. The administrators enabled a parameter of the virus scan program to automatically clean the virus-infected files. The virus scanner detected an instance of the CAP macro virus in a mail attachment WITHIN the Exchange database and proceeded to "clean" the file by performing an in-place modification on it. As a result the database was corrupted, users could not access their mail, and subsequent attempts to repair the database using the facilities provided by Exchange failed. Eventually the database was recovered from a backup resulting in lost e-mail messages. There are many lessons that can be drawn from this story; I would like to emphasise the risks of proprietary, opaque, or gratuitously complicated file formats such as those used by Microsoft Word documents, and the Exchange database. Architecting and implementing an efficient, extensible, and functional file format and interface can be difficult and expensive. However, the cost is most cases justified the resulting robustness, openness, usability, and extensibility of the system.

Diomidis Spinellis, University of the Aegean

⚡ MIME-Messages: quoted-printable chars in URLs

Christoph Conrad <Christoph.Conrad@post.rwth-aachen.de>

17 May 1999 07:19:56 +0200

Recently I made a request for an X509-certificate. The certification authority (CA) mailed me an URL for fetching my certificate, but it didn't work. It looked like ([...] parts are omitted by me):

[http://\[...\]CertIdentifierW746](http://[...]CertIdentifierW746)

So I wrote back to them and they answered that the last five digits are five seven seven four six, before the equal sign. I realized that this is a problem with MIME quoted-printable handling.

The real URL was:

[http://\[...\]CertIdentifier=57746](http://[...]CertIdentifier=57746)

"=57" is also a quoted printable char and means "character with value 0x57", this is a 'W'!

christoph.conrad@post.rwth-aachen.de

⚡ New-fangled petrol pumps

Ian Chard <ian@tanagra.demon.co.uk>

Thu, 13 May 1999 21:50:38 +0100 (BST)

I filled my car up with petrol today with one of these new-fangled petrol pumps that lets you stick your credit/debit card in, fill up your car and then drive away without having to queue up in the shop. I didn't really trust the pump (and I thought the poorly trained staff might think that I was just driving away without paying), so I asked it for a receipt. I

reached under the pump (where the printer is), grabbed the receipt, and drove away.

When I got home, I fished the receipt out of my pocket, and it struck me that the 28 quid I had been charged was rather more than my car could hold.

"Hmm," I thought, "maybe the prices have gone up". I then noticed that the card type was "MASTERCARD", which I don't have. "Hmm," I thought, "maybe it just represents Switch (my card type) as Mastercard. Then I noticed that the first digit of the (full) card number on the receipt was a 5, whereas mine was a 6. Then the penny dropped.

The printer took rather longer than I thought to print the receipt. What I got was someone else's receipt, with their full credit card number and expiry date. To my horror, I also realised that the next customer will get my card number and expiry date. Alas, it was now 30 minutes later, and my details are almost certainly in someone else's pocket.

The RISK here is not only that old adage about not printing the full card number when the last five digits will do. I wouldn't have had a problem if the thing had said "PRINTING PLEASE WAIT". What it did say was "PLEASE TAKE RECEIPT FROM BELOW PUMP". I looked, saw a piece of paper, and took it.

Ian Chard, Sheriffmuir <ian@tanagra.demon.co.uk> +44 976 249081
<http://www.tanagra.demon.co.uk>

⚡ Re: C compilers vs editors: WYSI NOT ALWAYS WYG (Graifer, [RISKS-20.39](#))

"Roy O. Wright" <royw@cisco.com>
Mon, 17 May 1999 17:02:06 -0500

In MS Visual J++, Microsoft will sometimes use a single carriage return as a line terminator. As pointed out by Daniel Graifer, this can introduce bugs when moving the source code to a different compiler - EVEN ON THE SAME PLATFORM (ex. Semantic's Visual Cafe and the Sun's Java SDK on MS Windows) This looks like either an attempt to lock a developer into one set of tools or very sloppy design.

The two workarounds I have found are to either load the source file into an editor that recognized "\n", "\r", & "\r\n" as line terminators (ex. PFE) then resave the file, or to write a filter to handle the translation.

Roy Wright, Cisco Systems royw@cisco.com 1-512-378-1234

⚡ Re: Wrong e-mail address (Wampler, [RISKS-20.39](#))

Andrew J Klossner <andrew@pogo.WV.TEK.COM>
Mon, 17 May 1999 16:36:17 -0700

All the risks that Bruce Wampler mentions for misaddressed e-mail have been present for centuries with misaddressed paper mail. Mangle one digit of a street address and your envelope can quietly go to the wrong place. It's then up to the good graces of the inadvertent recipient to

reroute it and to
respect its confidentiality.

The only difference I note is that important but misaddressed paper mail has a noteworthy appearance to distinguish it from bulk commercial advertisements, and is therefore less likely than e-mail to be discarded unnoticed.

Andrew Klossner (andrew@pogo.wv.tek.com)

⚡ Re: Risks of 3-letter user IDs (Yurman, [RISKS-20.39](#))

<Forbes_Thayne@emc.com>

Mon, 17 May 1999 12:28:40 -0400

It's worse than he thinks. First, I spoke with a friend who works at Hotmail and they currently have about 43 million subscribers. Surprisingly, about 1/3 log in every day. Assuming yahoo! and the rest are in the same ballpark, then Dan is off by an order of magnitude. Furthermore, people at these sites frequently get mail that was meant for the same username at another site. I.e. jsmith@hotmail gets mail meant for jsmith@yahoo.com. Their friends just can't remember what site they are at. (I have this problem with my kids, who all have free accounts SOMEwhere). Lastly, I would have thought that I could get an account with my name (thayne) but could not. I got forbes_thayne, but was surprised to learn that there is actually someone else on the net with the same combination of slightly

unusual names. I guess the lesson is that when you are dealing with millions of monkeys, anything is possible.

🔥 Dimwitted naughty-word filtering lives...

Daniel Rutter <drutter@curie.dialix.com.au>

Mon, 17 May 1999 17:24:45 +1000

I'm a subscriber to the Healthfraud discussion list (e-mail healthfraud-help@ssr.com for info), and every now and then get a warning e-mail from the Healthfraud ezmlm program telling me that messages to me have been bouncing, with the usual note that if the warning bounces too I'll be unsubscribed.

Often, the bounces are because my mailbox has been filled. My ISP here in Australia, Dialix (<http://www.dialix.com.au/>), allows its users only a 1Mb mailbox, which is OK with me because I check mail often and can access the local Dialix mail server much faster than the other couple of servers available to me. If a friend decides to send me a monster AVI file, though, a few messages will bounce before I clear the blockage.

Other bounces, though, are because of "suspicious keywords in FROM:", according to the Dialix mail server error message; some source e-mail addresses don't pass muster with the server. For this reason, I will of course never see the error messages myself unless something, like ezmlm or a human with a different e-mail address from the one that bounces,

brings them
to my attention. I have just discovered that these "suspicious
keywords" are
defined to include dirty words, even if these words are
coincidentally
included in an innocuous non-spam e-mail address, on the
assumption that any
e-mail address with a dirty word in it must be from a spammer
spruiking a
sex site, or some such.

So, for example, messages to the Healthfraud list from a retired
nurse with
the e-mail address nursex@... never made it to me. I presume e-
mail from
people called Frederick Uckham or Shirley Travis might not make
it, either,
if their e-mail addresses were composited from their names in an
unfortunate
way. I have no way of knowing how much valid e-mail has been
bounced by this
this over-inclusive, misguided "anti-spam" system.

Dialix provides absolutely no notification for its users about
the existence
of the system. I didn't even know it existed until a Dialix
support person
e-mailed me with the news that he'd removed "sex" from the
exclusion list
for the mail server at my Dialix point of presence, and was
still trying
to FIND the master exclusion list!

The RISK - don't assume that your ISP isn't doing stupid, STUPID
things just
because they don't say they are, and don't get cocky about the
reliability
of e-mail. Dimwitted system administrators can silently zot your
e-mail
better than any random Internet problem.

Daniel Rutter - DNRC Gadget Wrangler [http://www.fromorbit.com/
drutter/](http://www.fromorbit.com/drutter/)

<http://www.dansdata.com/> - in-depth hardware reviews and more!

🔥 REVIEW: "Removing the Spam", Geoff Mulligan

Rob Slade <rslade@sprint.ca>

Mon, 17 May 1999 10:57:05 -0800

BKRMSPAM.RVW 990328

"Removing the Spam", Geoff Mulligan, 1999, 0-201-37957-0,
U\$19.95/C\$29.95

%A Geoff Mulligan

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8

%D 1999

%G 0-201-37957-0

%I Addison-Wesley Publishing Co.

%O U\$19.95/C\$29.95 416-447-5101 fax: 416-443-0948 bkexpress@aw.
com

%P 190 p.

%T "Removing the Spam: Email Processing and Filtering"

This book is intended for the system manager, rather than the end user.

More specifically, it is aimed at the mail administrator for an ISP

(Internet Service Provider) or corporate network. Slightly unfortunate is

the fact that it becomes more particular still, being of greatest use to

those running UNIX, sendmail, ProcMail, and either Majordomo or SmartList.

Regardless of system expression, anti-spam configuration is, as Mulligan

points out, important for two reasons. The lesser of the two concerns is

the most obvious: that of restricting the amount of spam reaching your own

users. The more vital is that by failing to restrict the

possible abuse of your system by spammers, and particularly by permitting unrestricted relays, you face the increasing possibility of becoming blacklisted, and therefore hampering the legitimate use of the net by your clients.

Chapter one is an excellent overview of electronic mail. It is concise, complete, and accurate. Newcomers to the field will find not only a conceptual foundation for all the aspects of Internet e-mail, but also pointers to other references. Professionals will find fast access to a number of details that need to be addressed on a fairly frequent basis. The main theme, of course, is how spam uses the functions of e-mail systems, and how it can be impeded, with as little impact as possible on normal communications. A good framework is presented in this chapter, with a number of references to spam-fighting resources. If I were to make one suggestion, it would be to increase the number of examples of forged e-mail headers, and how to dissect them.

Chapter two describes sendmail, and goes into sufficient detail for interested people to obtain it and start using it. At that point, the text concentrates on barriers to spam, such as restriction of relaying and the access database. Administrators using sendmail will find this a quick guide to basic functions.

ProcMail has a variety of functions, and most of chapter three looks at the number of uses it can have. The spam filtering section is relatively brief,

but provides some recipes, and directions to other ProcMail based filters.

Again, sysadmins can use this as a quick start for basic mail processing.

Chapter four doesn't have a lot to say about spam, but it does review the proper setup of mailing lists, which can have a significant impact in reducing unwanted mail.

This book should be required reading for all mail administrators. The usefulness is not restricted to spam, since admins will be able to find brief discussions of a variety of common mail problems. As Mulligan notes, the fewer improperly configured mail servers there are out there, the more constricted spam sites will become, until at last they can be eliminated altogether. While the details of managing other mail server programs may not match those given in the book, the functions should be available, and should be turned on. If the functions aren't available, perhaps it's time you got some new software.

copyright Robert M. Slade, 1999 BKRMSPPAM.RVW 990328
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

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



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 41

Sunday 23 May 1999

Contents

- [Re: Biometric risks](#)
 - [Dan Wallach](#)
 - [Fred Herr](#)
 - [Dan Wallach reponding to James L. Cambier](#)
 - [Paul Lewis Gittins](#)
- [Costly fight about party software](#)
 - [Debora Weber-Wulff](#)
- [Embedded NT ...](#)
 - [Jeremy Epstein](#)
- [Vulnerability in Windows SSL server and common browsers](#)
 - [Chris Cowley](#)
- [Buggier than thou ... Wiretapping](#)
 - [Mike Williams](#)
- [Y1.K9](#)
 - [Mark Brader](#)
- [JAVA language definition](#)
 - [Craig DeForest](#)
- [Documentation for vapor](#)
 - [Seth Gordon](#)
- [Risks of aliasing webservers](#)
 - [Tim Panton](#)

● [May you live in interesting times, or What excites bankers](#)

[Mark Brader](#)

● [REVIEW: "Digital Democracy", Cynthia J. Alexander/Leslie A. Pal](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

🔥 **Re: Biometric risks ([RISKS-20.40](#))**

Dan Wallach <dwallach@cs.rice.edu>

Wed, 19 May 1999 20:01:11 -0500

A few clarifications on my last post.

- I mixed up iris and retina scans. The iris is the thing in front of your eye with the pretty colors. The retina is the thing in the back with the photoreceptors. Both are useful for identification, but the iris is somewhat less difficult to scan. Bank United of Texas intends to do iris scans.

- Two companies who are apparently big into eye-identification are Sensor [1] and IriScan [2]. The latter site has more depth in its description of the technology. One private e-mail I received described that modern ATM machines from Diebold and NCR run Windows NT (*sigh*) and allow third parties to integrate their own security measures.

- As biometrics go, iris scans seem to be pretty good. I'm willing to believe vendor claims of high discrimination and low error rates. In particular, [3] claims that the system can be designed to have an error rate

of approximately 1 in a million (both false accepts and rejects). There is a tradeoff where the designer can choose to decrease the odds of a false accept in exchange for increasing the odds of a false reject. One such stated data point would have one in 22700 customers falsely rejected in return for a one in 10^{11} false accept rate. "Authentication failed. Please try again."

- Claims that iris biometrics cannot be copied or spoofed seem less believable. Once I've got a good photograph of your iris, I should be able to (with some expense) construct an artificial eye that matches the original. Vendors claim recognition times of 2-4 seconds. That's how long you hold your styrofoam head in front of the machine. [3] mentions various other spectral scans (i.e., infrared light) that might distinguish a styrofoam dummy from an actual head and a glass eye from a real eye. I'm sure this stuff works great, but again will be broken in due course.

- I've received some interesting private e-mail on this subject. There are some people who don't have irises (300 children born this way per year in the U.S., says one person preferring to remain anonymous). One issue with pure biometric authentication is dealing with the non-zero number of people who don't happen to *have* your preferred biometric.

- Both companies seem to be marketing their products as the only form of authentication you need. This is my strongest complaint. I could support

the use of a smartcard as the primary identification and the biometric as a replacement for PINs or passwords. That would be sensible for banking applications and would help quash any desires for evil-doers to try beating the system. Also, for the biometrically-challenged, their cards could be coded in such a way as to indicate the customer is a special case for the system. Indeed, I find it hard to imagine my bank not wanting to keep a piece of plastic in my wallet with their name on it.

- Lastly, we haven't even begun to discuss the risks that occur when an industrious bank officer physically hacks the ATM. If the ATM hacker need only intercept the video camera wires, a quite nasty attack could be developed which nicely generates perfect "evidence" that a transaction occurred. Conversely, a crypto smartcard could go great distances in eliminating the ease of such an insider attack. (Not that smartcards don't have their own problems, for example, differential power analysis [4].)

Dan Wallach, Rice University

[1] <http://www.sensar.com/products/products.stm>

[2] <http://www.iriscan.com/technology.htm>

[3] <http://www.iriscan.com/basis.htm>

[4] <http://www.cryptography.com/dpa/>

✉ Re: Biometric Risks (Wallach, [RISKS-20.40](#))

"Herr, Fred K" <Fred.Herr@unisys.com>

Wed, 19 May 1999 14:38:42 -0400

[Fred's first 4 points were more or less covered by Dan's message,

which he send before I had sent him Fred's. I have removed them. PGN]

5. The same technology recently completed a pilot with ATMs in Swindon, UK, where it apparently generated high levels of satisfaction and enthusiasm.

Biometrics are pretty well established by now, as most anyone who attended the CardTech/SecurTech show in Chicago last week can testify. Most people who understand it are not afraid of the technology itself.

The legitimate Risk is how well will the biometric user, Bank United in this case, protect the biometric data. As a bank, I would expect them to provide the same level of protection they give to their customers' names, account numbers, balances, transaction histories, etc.

Movies that show bad guys cutting out eyeballs to defeat "biometric" security systems may provide cheap thrills and grist for the alarmists, but they bear little relation to the realities of biometrics today. My great grandmother may have been afraid to have her house wired for electricity, but I suspect Dan knows enough about that technology not to panic. I hope he, and others with equivalent understanding of biometrics, will spend a little time investigating. www.biometrics.org is a great place to start.

Privacy! You want privacy?! How about the medical testing company that

uses biometrics to insure their clients' COMPLETE anonymity.
They don't
even take your name and address. Just your biometric. Only you
can get
your test results because the key you use to get them is that
same
biometric.

Yes, biometrics can be part of systems that threaten privacy,
but they have
the potential to do more good than harm. Check out www.ibia.org.

Fred Herr

✉ Re: Biometric Risks (Wallach, [RISKS-20.40](#))

Dan Wallach <dwallach@cs.rice.edu>

Thu, 20 May 1999 15:28:11 -0500

Wow, my post really touched a nerve! Here's a note from
IriScan's VP of
Technology.

P.S. Geez, if I knew I was going to stir up this much mud...
Dan

Date: Thu, 20 May 1999 15:35:14 -0400

To: Dan Wallach <dwallach@cs.rice.edu>

From: "James L. Cambier" <jcambier@iriscan.com>

Subject: Re: Biometric Risks

Dear Mr. Wallach:

I am writing in response to your "Biometric Risks" article in
[RISKS-20.40](#),
18 May 1999.

First, to relieve some confusion. The biometric technology
being evaluated

by Bank United is IRIS recognition, not RETINA scanning. The iris recognition equipment used in the Diebold ATM machines (and those of several other ATM manufacturers) is supplied by Sensar (www.sensar.com), which in turn is a licensee of IriScan, Inc. (www.iriscan.com), which developed and holds worldwide rights to the core iris recognition technology. The significant differences between the capabilities, performance, and user friendliness of iris vs. retina imaging are detailed in our website, www.iriscan.com.

I would offer several counters to the assertions in your article. Relying on a single authentication factor, "something you are", is NOT a disaster if the biometric used is based on the human iris, which offers profoundly higher information content and, with appropriate algorithms, several orders of magnitude lower false accept and false reject rates than any other biometric. This is attested by numerous independent studies and widely accepted within the biometrics industry. Iris recognition equipment manufactured by IriScan has been in use in government, industrial, corrections, banking, and other facilities for at least five years with resounding success. And unlike other biometrics, iris recognition has sufficiently low error rates that it can be used in large scale identification (as opposed to verification) applications successfully. Hence there is no need for usernames, passwords, tokens, etc. Identity is determined solely from the iris template. And in the millions of iris

recognitions that have been conducted by evaluators and customers over the last ten years, we have NEVER experienced a false accept event.

The iris recognition system used by Bank United does not transmit images or maintain them in any archival storage. Each captured image is immediately processed to generate a proprietary, highly unique 512-byte IrisCode(TM) template then the image is deleted. The template is encrypted (using industry standard encryption algorithms) before it is transmitted to the bank for authentication.

Needless to say, the iris recognition technology includes countermeasures to guard against attempts to deceive the system with photographs or other devices. And, finally, the postscript at the end of your article about "potential eye damage from miscalibrated units" is unfounded and irresponsible. The illumination used by this and other iris recognition devices is extremely low level, near-infrared illumination that is incapable of producing energy levels greater than several orders of magnitude below commonly accepted damage thresholds for the eye.

[Yes, I was thinking of the Therac 25, where it was falsely believed that

the system could not harm the patient. I realize that well implemented

iris scanning might not have that risk, but for long-time readers of

RISKS, believing in such certainties is often itself a huge risk. PGN]

Please feel free to contact me if you have any questions or comments.

James L. Cambier, Ph.D., VP Technology Development, Chief
Technology Officer
IriScan, Inc. 9 East Stow Road, Suite F Marlton, NJ 08053-3159
609-797-6890

✶ **Re: [Risks Digest 20.40](#), Iris Scanning ATMs**

Paul Lewis Gittins <plg101@york.ac.uk>

Fri, 21 May 1999 23:52:05 +0100

RE: Iris Scanning ATM'S

Further to the recent article, I hope that any bank implementing the iris scanning systems will not be relying on this as the sole authentication method. There is an inherent problem, in that this further disadvantages some people with visual disabilities. Visually impaired users who wish to use atms have little enough thought from interface designers as it is, without further problems in hampering the UI. Suppose the user has no iris that can be scanned, will a pin number still suffice? OK, it may be a small number of users, but the user group does still exist. With banks pushing more and more services out to atms and remote access, it must only be a consideration that users must not have further hamperings in using the system....

I remember a quote from my old tutor, regarding Drexel (sp?) University saying that all undergraduates should buy a Mac to do their courses - what they were implying was that blind users need not apply.....

Paul

✦ Costly fight about party software

Debora Weber-Wulff <weberwu@tfh-berlin.de>

Thu, 13 May 1999 10:31:41 +0200

[excerpted and translated from "Der Tagesspiegel", 1999-05-12, p. 5]

The central administration of the SPD party, the major coalition partner in Germany, has no idea who belongs to the party or if they are up to date with their dues. The problem is software that was delivered by the large German software company SAP, says the SPD, who employed a company in Hamburg to document the problems in September 1998. This company notes: "Not one of the larger batch runs has been free from problems, programming errors, unexpected terminations or needed corrections."

SAP retorts: "The SPD ordered a VW Beetle but expects us to deliver a Daimler [Mercedes-Benz]". The SPD bites back: "We would be happy to have software that runs like the Beetle, but we have had to correct disastrous errors ourselves". [No word on what the cause of the problems is.]

While the fight, purported to be about the 35 million DM price for the software (about 19 million \$), rages, the SPD has no way of knowing exactly how many members it has [or if there are enough DM coming in from outstanding dues to pay the lawyers!]. -- Prof. Dr. Debora

Weber-Wulff TFH

Berlin, FB Informatik Luxemburger Str. 10, 13353 Berlin, Germany
weberwu@tfh-berlin.de <http://www.tfh-berlin.de/~weberwu>

✶ Embedded NT... (in case you don't have enough to worry about already)

"Epstein, Jeremy" <Jeremy_Epstein@NAI.com>

Fri, 21 May 1999 07:29:45 -0700

One of the articles about the well-reported link between Xerox and Microsoft (in which Xerox will use "embedded NT" in its copiers and Microsoft will license certain Xerox web technologies) had an interesting comment. John Markoff reports in *_The New York Times_* May 19th edition that "although the reliability of Windows NT has been questioned in so-called mission-critical industrial applications, the company has succeeded in persuading hardware developers to use it in a wide variety of devices, ranging from point-of-sale systems to computer routers and airline avionics." The article also mentions the infamous 1997 incident where the USS Yorktown was left dead in the water due to a failure related to NT (although it's still unclear whether it was a flaw in NT itself).

Makes me wish for the good old days of the early Airbus fly-by-wire systems.....

--Jeremy

⚡ Vulnerability in Windows SSL server and common browsers

Chris Cowley <ccowley@grok.co.uk>

Fri, 21 May 1999 14:39:00 GMT

Some time ago, I downloaded a trial version of an SSL web server product for Windows NT called 'Alibaba 2.0' for evaluation as a possible SSL solution. I eventually made a decision to use another product, but I ended up using an RSA key pair generated by Alibaba's 'genkey' utility (which is based on the popular SSLeay toolkit).

Whilst recently examining the keys generated by 'genkey' using tools shipped as part of the SSLeay distribution, I discovered what I believe to be a serious flaw:-

The 'genkey' utility erroneously generates a private key with an exponent of '1'. This results in null security since the RSA public key associated with a private exponent of '1' is also '1', with the effect that the session key for each SSL session to a server running 'Alibaba' is sent in the clear.

The result of this vulnerability is that 'secure' web sites that use keys generated by the 'genkey' utility provided with Alibaba 2.0 do not provide any security. Such sites are susceptible to having their transactions snooped by a third party, or falsified by man-in-the-middle attacks.

A further interesting discovery is that both Netscape Navigator and Internet Explorer will happily let the user interact with SSL web sites

which have an RSA public key exponent of '1' without bringing the user's attention to the fact that such transactions are, in fact, entirely insecure.

Chris Cowley, Grok Developments Ltd <http://www.grok.co.uk/>

⚡ Buggier than thou ... Wiretapping

Mike <John.Michael.Williams@Computer.org>

Fri, 21 May 1999 09:20:47 -0400

Electronic Wiretaps on Wireless Devices Outnumber Those On Wireline Phones

An annual report by the Administrative Office of the U.S. Courts reveals the number of electronic wiretaps on wireless phones and other wireless devices has more than tripled in the past year. (USA Today <http://www.usatoday.com/life/cyber/tech/ctf213.htm>)

⚡ Y1.9K

Mark Brader <msbrader@interlog.com>

Tue, 18 May 1999 15:47:42 -0400 (EDT)

[From Mark after forwarding to him from David M. Sherman. PGN]

> J.J. McVeigh wrote:

> >
> >]]]]]] EMPEROR HIROHITO'S DEATH CAUSES SOFTWARE PROBLEMS
> > []]]]]
> > (1/18/1989)
> > [From Pavan Sahgal, ``Automation at the "Big Four" Securities
> > Firms'', Wall Street Computer Review, January 1989, p. 23]

> >
> > [Kindly uploaded by Freeman 10602PANC]
> >
> > Under Japanese custom, when a new emperor is crowned, his
> > reign or era is marked by a title that appears on all
records in
> > the country. [Hirohito's era was called Showa, or peace.]
> > [E]xecutives at Tokyo's leading securities firms were
> > chagrined to discover that the computer programmers who wrote
> > accounting, recordkeeping and customer billing systems
software
> > in recent years created inflexible systems. They did not
> > envisage that someday Japan would have a new emperor, and his
> > reign would mark the start of a new era requiring records and
> > statements to reflect that.
> > The dilemma is comparable to having a system that won't
change
> > from 1988 to 1989. The programmers had overlooked an
essential
> > detail that obviously has widespread fundamental
implications.
> > Even worse, a new generation was sadly out of touch with
custom
> > and the saying, Koin ya no-goto she [acute accent over e] (A
> > lifetime goes like an arrow).
> >
> > * * *
> > <http://www.powerup.com.au/~dominion/ff/k14.htm>
>
> David M. Sherman, LLB, LLM, Tax Author & Consultant
> ds@davidsherman.ca <http://www.davidsherman.ca>

⚡ JAVA language definition (Was Re: C Compilers vs editors)

<craig@deforest.org>

Wed, 19 May 1999 10:33:20 -0700

Roy Wright and Daniel Graifer have pointed out that MS Visual J+
+ sometimes

uses a single return carriage to end a line, breaking some compilers. Roy suggested that the problem is either "an attempt to lock a developer into one set of tools or very sloppy design".

I forwarded the note on to my friend Josh Engel, who just finished writing a large monograph on Java. He sent me the following snippet:

>From the Java language specification:

>

>>3.4 Line Terminators

>> ...

>>LineTerminator:

>>

>> the ASCII LF character, also known as "newline"

>> the ASCII CR character, also known as "return"

>> the ASCII CR character followed by the ASCII LF character

>>

>>Lines are terminated by the ASCII characters CR, or LF, or CR LF. The two

>>characters CR immediately followed by LF are counted as one line

>>terminator, not two. The result is a sequence of line terminators and input

>>characters, which are the terminal symbols for the third step in the

>>tokenization process.

>>

>*****

>As I read this, Visual J++ is correct. A CR by itself is a line terminator.

>

>If Cafe and the JDK fail to recognize CR by itself as a line terminator,

>then they are not in compliance with the spec and must be corrected.

So M\$ may indeed be trying to "embrace and break", but for once they're staying wholly within their allowed spec. (The Java spec in

this case is
the document co-authored by GLS, not some Redmond-spawned
variant.)

The RISK? If you break enough specs, eventually people will
assume that all
software incompatibility is your fault.

[I'm guessing that Craig's last name might be DeForest.
If not, I am guilty of DeForestation by adding two extra
lines. PGN]

🔥 Documentation for vapor

"Seth Gordon" <sgordon@kenan.com>
Wed, 19 May 1999 13:32:07 -0400

A few weeks back, our company upgraded all of our PCs to use the
latest
version of Microsoft Office. Aside from experimenting with
Outlook, I
ignored the upgrade, since our group uses FrameMaker for all of
the
documentation we write. Now, I have to produce templates in
Microsoft Word,
so that people in our company who have Word and not FrameMaker
can produce a
document that is formatted like our standard documentation.

The upgrade had not come with a manual, so I went down to the
local nerd
bookstore in search of books on Word, and one of the items on
the shelf was
Running Microsoft Word 2000 (Microsoft Press). I dimly
recalled people
referring to my version of Office as "Office 97", but I figured
that the
"Office 2000" label might be a marketing gimmick and not a
distinct version.
The windows in the screen shots looked like the windows I had

seen using the program, so I bought the book.

After a couple days wrestling with the program, the manual, and Microsoft's Web pages, I discovered that:

- (1) Word 97 SR-2 is not, in fact, Word 2000.
- (2) Word 2000 hasn't been released yet.

OK, I erred by not looking up my version number before going on this shopping trip, but ... what's the point of selling a nine-hundred-page manual for a program that hasn't been released yet?

seth gordon == documentation group, kenan systems corp.

⚡ Risks of aliasing webservers

Tim Panton <thp@westhawk.co.uk>

Thu, 20 May 1999 16:15:59 +0100

I've just been browsing the Trustwise web site - they sell Verisign certificates for us UK users.

They seem to be owned by BT, which has resulted in an entertaining problem

When I opened <https://www.trustwise.bt.com/ServerIdCentre.html> I get a message from IE saying:

<QUOTE>

A secure connection with this site can not be verified. Would you still like to proceed ?

The certificate you are viewing does not match the name of the site you are

trying to view.
</QUOTE>

Viewing the certificate shows that it was assigned to www.trustwise.com .
When I altered the URL, I got a correct page.

Looking in the DNS, I see that they have the same IP address(es).

www.trustwise.com internet address = 193.113.157.254
www.trustwise.com internet address = 193.113.157.253

www.trustwise.bt.com internet address = 193.113.157.254
www.trustwise.bt.com internet address = 193.113.157.253

If a company selling certificates can't get it right - what hope have the rest of us.

Tim Panton <thp@westhawk.co.uk>, Java consultant/implementor
Westhawk Ltd
Westhawk Ltd, Albion Wharf, Albion St, Manchester M1 5LN +44
1612370660

⚡ May you live in interesting times, or What excites bankers

<msbrader@interlog.com>
Tue, 18 May 1999 16:38:01 -0400 (EDT)

In a brochure on their Y2K readiness, the Bank of Montreal writes:

Seeing the calendar change to the Year 2000 will be an exciting event.

I certainly hope it doesn't prove "exciting"!

Mark Brader, Toronto
msbrader@interlog.com

Carpe pecuniam!
--Roger L. Smith

⚡ REVIEW: "Digital Democracy", Cynthia J. Alexander/Leslie A. Pal

Rob Slade <rslade@sprint.ca>

Tue, 18 May 1999 08:40:11 -0800

BKDGTLDM.RVW 990326

"Digital Democracy", Cynthia J. Alexander/Leslie A. Pal, 1998,
0-19-541359-8, U\$26.50

%E Cynthia J. Alexander

%E Leslie A. Pal

%C 70 Wynford Drive, Don Mills, Ontario M3C 1J9

%D 1998

%G 0-19-541359-8

%I Oxford University Press

%O U\$26.50 212-679-7300

%P 237 p.

%T "Digital Democracy: Policy and Politics in the Wired World"

As a techie, I more comfortable with the "hard" sciences with provable outcomes, such as the "running code" (1) of the Internet. However, as one interested in the social aspects of the net, I have to respect the softer sciences, since without "rough consensus" (2) there would be neither protocol standards, nor the real heart of the communications that goes on. As Dimwiddy and Bunkum state (3), though, PoliSci is so soft as to be positively mushy.

Right from the beginning (4) the text is heavily larded with footnotes, which sometimes threaten to overpower the essays they are supposed to support (5). Oddly, though, these footnotes do not give

any impression of the strength of the material in the book, quite the contrary. Instead, they tend to lend credence to the statement that 94.3% of all statistics are made up on the spot (6). The content of the book tends to be strangely unformed, with statements ranging between unsupported bombast that we are simply assumed to accept, to citations of studies without much discussion of relevance or validity.

After an introduction, there is a piece on "social forces in the hypermedia environment" that seems to want to talk about economics, a discussion of national security, and something looking at the national or global information infrastructure. None of these pieces, and, indeed, nothing in the book, seems to have any real idea of the technology involved, or the implications of the technology. A look at women on the net states that "Few will argue the impact of written language or--many centuries later--the printing press in shaping new societies" (7) while blithely ignoring the fact that we have very little idea of what those impacts might have been. Leslie Pal's own contribution, examining the outcry over the Communications Decency Act, seems to have the greatest understanding of modern communications systems, but even there (8) does not comprehend that the technical aspects of "flooding" algorithms and dynamic rerouting were what forced commercial services to lobby against the bill.

The paper on teledemocracy bemoans the fact that lack of a touch tone phone disenfranchises a massive 5% of the population (9), while ignoring as insignificant a 12% disparity in polling results (10). His lauding of Ted White's telephone polling (11) was of

particular

interest to me, since I live in White's riding and a) didn't get a pin, b) could have reproduced White's polling system using local technology at far lower cost to both constituents and the government (12).

There is a pedestrian piece on intellectual property. Then there is the mandatory article on pornography. (Can we have a Rimm shot? Thank you.) The Rimm "study" (13), and another equally suspect, categorize a bunch of feeble peechers, and we are then told that there is a clear benefit for regulation of pornography (14).

The essay on privacy takes for granted that you cannot have freedom without privacy (15), ignoring items like David Brin's "The Transparent Society" which proposes a remarkably free environment almost completely devoid of privacy (16). The article also decries identification numbers of all types, and then goes on (17) to laud public key encryption, seemingly unaware that a public key is a number.

Neither the discussion of health care nor that of indigenous people really looks at social aspects of the technology.

This seems to be my week for dumping on compatriots (18). However, my rabid nationalism does not extend so far as to defend those resident in my country when they don't know what they are talking about, and this book seems to be almost completely devoid of experience of the technology under examination.

(1) Dave Clark (of MIT), IETF Conference, 1992

(2) *ibid*

(3) I made them up, of course.

(4) Well, I suppose not; there are no footnotes in the acknowledgement; but the first one comes in the second paragraph of the preface on page xii.

(5) They never actually do.

(6) This figure is embedded in one of my brother's sigblocks: I think he made it up.

(7) p. 88

(8) p. 111

(9) p. 140

(10) p. 135

(11) p. 136

(12) White used Maritime T&T, had to spend \$11,000 setting up a single poll, and it cost people \$1.95 per time to vote. A PC based system could have, at the time, been established for about \$5,000 altogether, and could have been reused at any time for further polling.

(13) lucky, eh?

(14) p. 176. I'm not exactly on the side of pornography, but there are a few steps missing in the proof, here.

(15) p. 181

(16) cf. BKTRASOC.RVW

(17) p. 187

(18) See also "Roadkill on the Information Highway" (BKRKOTIH.RVW)

copyright Robert M. Slade, 1999 BKDGTLDM.RVW 990326
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

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



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 42

Tuesday 25 May 1999

Contents

- [Breakdown leaves swimmers in the cold](#)
[Paul Oldham](#)
- [Professional hazard in lightning monitoring](#)
[Amos Shapir](#)
- [Airport radar comes under scrutiny](#)
[Doneel Edelson](#)
- [Hospital delivery robot blocks exit from elevator](#)
[Lyle Gray](#)
- [Y2K testing on weather images](#)
[Amos Shapir](#)
- [German government criticizes own style in Word documents](#)
[Debora Weber-Wulff](#)
- [Summary of biometric responses](#)
[Dan Wallach](#)
- [Re: Biometrics](#)
[Dave Upton](#)
- [Eye swear, it was working yesterday!](#)
[Adam Shostack](#)
- [Addressing phenomenon: Once a Canadian, ...](#)
[Mich Kabay](#)

- [Security vulnerability in Netscape](#)
[Lindsay Marshall](#)
 - [Emperor Hirohito's death causes SW problems](#)
[Stuart Woodward](#)
 - [Re: JAVA language definition](#)
[Jim Thompson](#)
[Robin Landis](#)
 - [Microsoft "fixes" the MS Office macro virus vulnerability](#)
[Paul Walker](#)
 - [Embedded NT... in case you don't have enough to worry about already](#)
[Gregor Ronald](#)
 - [REVIEW: "Microsoft Windows NT 4.0 Security, Audit, and Control"](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Breakdown leaves swimmers in the cold

Paul Oldham <paul@the-hug.org>
Mon, 24 May 1999 17:38 +0100 (BST)

Cambridge Evening News of 24th May 1999 reports the following story:

Swimmers taking a dip in Ely's newly-refurbished Paradise Pool were stranded when a high-tech locker-system broke down, leaving many without their clothes and belongings.

Shivering swimmers were wrapped in silver foil blankets after the incident yesterday, when the electronic lockers shut down after a power failure.

People were forced to wait for an hour-and-a-half until mechanics arrived at the scene. Youngsters who had come by themselves were given money to

make a call home. Free drinks and food were also handed out.
New swimmers

were stopped from using the pool, which was closed for a short
time while
the problem was dealt with.

The system which replaces the "key and coin" scheme usually
found in
public pools means that swimmers can access their locker with
a tag fitted
with an electronic microchip.

The new and improved leisure pool, which recently underwent a
UKP1.9
million renovation, has only been open for little more than a
month.

Apart from wondering whether this risk had ever been considered
by either
the designers or the people who procured this system, one is
left wondering
what the benefit was on this system over the traditional key and
coin
scheme, which appears to work perfectly well at many pools in
the area and
has no failure mode which leaves every locker locked.

Paul Oldham, Milton, Cambridge, UK <http://the-hug.org/paul/>

[Perhaps the system was designed by the Davy Jones Locker
Company. PGN]

Professional hazard in lightning monitoring

<amos@nsof.co.il-n0spam>
24 May 1999 13:17:00 GMT

For the past few days, the European lightning strikes charts at
<http://www-imk.physik.uni-karlsruhe.de/~gmueller/metbest.html>

are showing an empty map, with the inscription: "Due to technical reasons (lightning strike) no lightning charts are available".

It doesn't say what part of the system was struck.

Amos Shapir, nSOF Parallel Software, Ltd., Givat-Hashlosha
48800, Israel
Tel: +972 3 9388551 Fax: +972 3 9388552

[Reminds me a little of lightning striking the launch pad at Wallops

Island that accidentally launched a missile that had been prepared to be

launched in order to test the effects of lightning. PGN]

⚡ Airport radar comes under scrutiny

"Edelson, Doneel" <doneeledelson@aciins.com>

Tue, 25 May 1999 12:03:31 -0400

For as many as a dozen times during an hour-and-a-quarter period during the midafternoon of 17 May 1999, repeated failures in a computer processor at the Philadelphia International Airport caused the radar-osaurus system to fail, losing partial data associated with each flight. The outage required air-traffic controllers to resort to the even older paper-slip backup system. As usual, the official spokesperson said ``There was no impact to safety.''

[Source: an article in USA Today, 23 May 1999, which noted that a power failure earlier in May had caused a 23-minute outage of radar scopes and radio contacts in the same place; PGN-ed]

⚡ Hospital delivery robot blocks exit from elevator

"Gray, Lyle" <Lyle@Quodata.Com>

Fri, 14 May 1999 18:21:07 -0400

While I was being transported by gurney to an operating room in February of 1998, a hospital delivery robot (essentially a large, automated supply cart) met the elevator when it arrived on the operating room floor.

The robot knew that the elevator was occupied, and instructed us to clear the way so that it could enter. However, as the elevator had a gurney in it, there was not enough room to clear the way. The robot would not back away from the elevator to let us out, and we could not close the elevator doors to try to go to a different floor, because the doors were being blocked by the robot.

Finally, a medical technician man-handled the robot out of the way so that the gurney could be pushed out of the elevator, leaving it to try to figure out its new orientation and try again.

The Risk? Not programming the robot to allow for a situation that must be common in its environment (gurneys in elevators).

Lyle H. Gray

⚡ Y2K testing on weather images

<amos@nsof.co.il>

Tue, 25 May 1999 15:29:14 IDT

There's a site at Nottingham U., UK, where weather satellite images are received from a geostationary satellite (Meteosat), timestamped and prepared in several different formats. (ftp.ccc.nottingham.ac.uk)

I download some images regularly off this site a few time a day. One morning last week, several images were missing; the next image available, was timestamped "FEB 28 2000, 2330" (though it seemed to be a current one). The next one was timestamped "FEB 28 2000, 2400". Oh well, back to the debuggers... (the rest of the images on that day had their correct timestamps).

Amos Shapir, nSOF Parallel Software, Ltd., Givat-Hashlosa 48800, Israel
Tel: +972 3 9388551 Fax: +972 3 9388552

[Perhaps they were running a Y2K leap-year experiment. PGN]

🔥 German government criticizes own style in Word documents

Debora Weber-Wulff <Debora.Weber_Wulff@te.mah.se>

Mon, 24 May 1999 16:42:37 +0200

My husband, a historian, downloaded a lot of official German government documents for a talk he is preparing on reunification. Many of the documents are in some Microsoft format or other. The most amusing one was stored in .doc format on their web pages in the proofreading version. That

is, one can see that they have replaced all references to DDR with Ost (East), and so on. A quick look at the properties of the file is hilarious: "The style of this file is stilted, pompous, noun-laden, non-concise and in general not useful. Must be rewritten!"

Interestingly enough, since no author is filled in in this field, Microsoft decides that I, as the license holder, am the author of the document. Other documents, for which no organisation is entered, believe that my organisation is responsible. The moral of the story: if you are using such products for net publication, make sure that there are no little surprises hiding in the text!

Prof. Dr. Debora Weber-Wulff, Technische Fachhochschule Berlin, FB, Informatik, 13353 Berlin, Germany <http://www.tfh-berlin.de/~weberwu/>

Summary of biometric responses

Dan Wallach <dwallach@cs.rice.edu>
Mon, 24 May 1999 19:21:16 -0500

Our esteemed moderator is up to his eyeballs in biometric responses and has asked me to look them over and make a summary. Here goes:

David Kinny [a] and C. Scott Ananian [b] mention possible issues with contact lenses and object to being required to remove them. According to Ananian, newer contacts have both color and texture on them (for

cosmetic

reasons, of course). IriScan claims to be able to deal with contact lenses but doesn't give precise details of how this works [1]. I would refer readers with these kinds of detailed technical questions to IriScan's Web pages.

Ananian discusses future generation contact lenses, which presumably will take us further away from natural-looking eyes. I imagine that, in the limit (say, reflective lenses), contacts would have to be removed to make a positive authentication.

Also writes Ananian:

```
> Finally, although we are assured that iris images are deleted
> immediately after processing, we all know the permanence of
data on
> today's digital hardware. If those images are swapped to disk
or
> ever written to a file during processing, a thief might
acquire not
> just one but *several* iris images with appropriate scrubwork
over
> the magnetic media. Combined with appropriate contact lens
> technology...
> --s
> [note that this opens up an interesting avenue regarding the
alleged
> 'irrevocability' of one's biometric; here's something I can
> (potentially) change at will, despite being an almost
inseparable
> part of the vison-corrected me]
```

The vendors would likely claim that no contact lens will allow you to assume somebody else's indentivity and they might be correct. However, if relatively opaque lenses become fashionably normal, the efficacy of iris scanners would

be greatly reduced.

Steve Feinstein [c] discusses the issue of 'cloning' someone in order to produce identical irises. Vendor studies of identical twins show that irises are truly personal -- the exact iris patterns form as a function of development, although certain gross features (i.e., color) are genetic.

William Leary [d] and Marcus Rowland [e] discuss scenarios whereby an ATM user is vulnerable during the 2-4 seconds they are being scanned. If you hear a noise behind you, you either look around (safety first, after all) and then restart the authentication later, or you resolutely stare forward, allowing an assailant a known time window where you are more vulnerable to a mugging. Given how current ATMs requires you to stare at the screen right now to follow their instructions, I don't think iris scanners exacerbate this problem.

Paul Czyzewski [f] mentions a general privacy concern, i.e., that iris scanners could be installed everywhere we currently have security cameras and might be able to scan your "involuntarily". This could be a big step toward an Orwellian future. As it stands today, the technology only seems to work under controlled circumstances. Unless the government bans sunglasses, you should be relatively safe well into the future.

Finally, Mark Hayman [g] brings up the scenario where current ATMs will, upon multiple bad PIN entries, "eat" your ATM card. Hopefully, iris-scanning ATMs will not employ an analogous strategy.

Dan Wallach, Rice University

[1] <http://www.iriscan.com/basis.htm>

[a] dnk@OMIT.cs.mu.OZ.AU

[b] cananian@lesser-magoo.lcs.mit.edu

[c] saf@netcom.com

[d] leary@emc.com

[e] mrowland@ffutures.demon.co.uk

[f] paulc@shell11.ba.best.com

[g] mjh@castle.on.ca

[Incidentally, Bruce Schneier makes some compelling arguments against

biometrics, although he is obviously for strong authentication. See

<http://www.counterpane.com/crypto-gram-9808.html#biometrics>

PGN]

Re: Biometrics

<Dave.Upton@dotrs.gov.au>

25 May 99 10:14:54 SST

What's the Problem?

My question at the top of this still stands. I know you can all answer that

and some of you have but when compared to what we have What is the problem?

The system we have now of easily duplicated cards with insecure PINs surely

has more proven risks than those posed by biometrics. Sure sometime in the

future security measures for these devices may well be compromised but by

then hopefully those measures will have moved on. Sure some people will be

"biometrically challenged" but are there not "ATM challenged"

people out
there now who are missing out?

If we wait for the perfect system the waiting will never end.
There are
risks but it seems to me not as many as with our current system
of cheques,
credit cards, ATM cards and PINs.

So again I ask, What is the problem?

Dave Upton <http://www.geocities.com/researchtriangle/1362>

⚡ Eye swear, it was working yesterday!

Adam Shostack <adam@netect.com>

Mon, 24 May 1999 09:26:40 -0400

One of the risks of a purely biometric system is that biometrics
are
sometimes destroyed in accidents. This is often a major concern
in hospital
patient tracking systems, since most of those accidents lead
directly to the
patient being brought to the hospital, where the alternate
lookup method
needs to be invoked. Interestingly, this risk is obvious to the
medical
industry, because of the scenarios which they examine when
designing their
systems.

I suspect that there will be alternate methods in place, if the
banks
deploying have realized that having only biometrics in their
ATMs may
violate the Americans with Disabilities act.

⚡ Addressing phenomenon: Once a Canadian, ...

Mich Kabay <mkabay@compuserve.com>

Mon, 24 May 1999 11:25:36 -0400

[From a recent letter clearly showing an Evil Plot to tar me with my
Canadian citizenship forever:]

Dear Dr Kabay:

This is in reference to the note you sent regarding your address in

Vermont. I can understand your dismay on seeing that Canada appears in

your address when you live in Vermont. Our new ... system has a slight

flaw in it at this time. Because you are a Canadian citizen our files

show Canada as your country. This ... triggers the word Canada to

appear in your address. I am assured this will be corrected shortly. ...

For the record, this illustrates

(1) a design flaw in which a hidden assumption comes to light with an exceptional case;

(2) bad quality assurance;

(3) the paucity in this database of Canadians who have moved to the USA.

M. E. Kabay, PhD, CISSP / Director of Education, ICSA, Inc.

<<http://www.icsa.net>>

⚡ Security vulnerability in Netscape

<Lindsay.Marshall@newcastle.ac.uk>

Tue, 25 May 1999 16:41:37 +0100 (GMT)

Netscape has a security vulnerability related to Javascript in a <TITLE> of a bookmarked page, which is executed with the privileges of the user when the bookmark file is next processed.

See <URL:<http://linuixtoday.com/stories/6211.html>> for more info.

⚡ Emperor Hirohito's death causes SW problems (Re: Y1.9K, R-20.41)

Stuart Woodward <stuart@gol.com>

Tue, 25 May 1999 16:15:53 +0900

I once worked on a software product for which an update was required to support the new Imperial Era name ("Heisei") after death the previous Emperor (a.k.a "Showa"). At the time I asked why the developers hadn't just put the Imperial names and dates into a ini file which could be edited after the death of the Emperor who was frankly getting on when the software was released.

The reply was that it had been thought of but by building this feature into the product it could have caused offense by publicly anticipating the death of Emperor.

Anyway, when he finally passed away, people continued to use the old Imperial era year for some time in conjunction with the new

until it was supported by software and printed on forms etc. In the month after the new era name was announced there were enormous sales of rubber stamps with the characters for the new era name.

And guess what, I bet in 99% of Japanese software applications the era name and start/end dates is still hard coded into the logic of the program as it is just a convenient format for display and never a basis for calculation which is done using the western date.

✂ Re: JAVA language definition (craig@deforest.org, [RISKS-20.41](#))

Jim Thompson <jim.thompson@pobox.com>

Mon, 24 May 1999 16:49:32 GMT

<craig@deforest.org> writes:

> Roy Wright and Daniel Graifer have pointed out that MS Visual J++
> sometimes uses a single return carriage to end a line,
breaking some
> compilers.

Actually, Daniel Graifer's original report concerned the Visual C/C++ suite, not J++. The problem reported was that the Microsoft Visual editor would display a single unix-style linefeed character <LF> as end-of-line, but that the integrated compiler was not treating the <LF> character as end-of-line. Thus, the compiled code did not match what the editor displayed, or what the

programmer expected.

This is not a failure to obey a standard; it is a failure of two related applications, the editor and the compiler, to treat the *same* input in a the *same* manner. It is all the more unfortunate because the two applications are "integrated", and should be consistent at least with each other. (They can't be consistent with the standard, because C++-style "//" comments in C code are nonstandard.)

Jim Thompson <jim.thompson@pobox.com>

🔥 Re: JAVA Language Definition ([RISKS-20.41](#))

<robin.landis@exim.gov>

Mon, 24 May 1999 09:50:22 -0400

How quickly we forget!

Twenty years ago it was PC/DOS vs mainframe and UNIX operating systems grumbling about this same issue. We still add the CRLF when converting from EBCDIC to ASCII as we pull data down from a mainframe to our PC network. Software companies DO create problems willfully for whatever purpose ... and sometimes they get double benefit for their efforts.

🔥 Microsoft "fixes" the MS Office macro virus vulnerability

"Walker, Paul (India)" <paul_walker@in.ml.com>

Tue, 25 May 1999 17:50:11 +0530

As a service to RISKS readers who have to deal with the problem of vulnerabilities in the MS Office software suite exploited by Macro Viruses, I direct you to...

<http://officeupdate.microsoft.com/downloadDetails/o2ksec.htm>

<quoted without permission>

The download file, O2ksec.exe, contains the Microsoft Office 2000 Macro

Security white paper. This white paper is a Word document that can be

opened by either Word 97 or Word 2000. The Microsoft Office 2000 Macro

Security white paper discusses how you can prevent the introduction of macro

viruses into your computer using Office 2000.

For example, Office 2000 introduces digital signatures to help users

distinguish legitimate code from undesirable code, such as viruses. If you

open an Office document and see a macro security warning with digital

signature information, you can feel reasonably confident that the person

(or corporation) who signed the macros wrote them. You can choose to trust

all macros signed by this person by checking the Trust all macros from

this source checkbox. From then on, when you open a document that contains

macros signed by this trusted source Office enables the macros without

showing a security warning for the document.

If you use the Office 2000 digital signature features as advised in this

white paper, you will not see annoying security warnings for any of the

macro solutions that you write or use. You will only see a security warning when it is justified; that is, when you open a document with unexpected macros or viruses.

Before you go rushing off to get this Word document, I would like to bring up the following points:

1/ the document comes as a self extracting and installing executable

(165 KB executable to install a 177 KB document into your "My Documents" directory... how thoughtful!).

We all know how no one could ever hack the MS Web site and replace the installation program with a Trojan to do additional tricks,

The document does not contain any macros, fortunately. At least someone was thinking a little ahead.

2/ the improved protection only comes if you upgrade to the next greatest and latest software

I don't know about you, but if I was a large corporation with a macro virus problem, I would resent having to do yet another upgrade just to get protection that should have been in the software in the first place.

3/ the process of signing and certification relies on trust.

I trust that when you sign your macros that you cannot in any possible way lose control of your private key. Your private key will be stored on your computer, which we all know that on a Windows based computer, is

completely
secure... well, let's not step off that bridge, shall we?

Fortunately, the document warns "Certificate owners should guard their
private keys carefully. Their reputations are on the line."

or shall we say that "their reputations are on-line"

With that warning, we all know that no one will overlook their security.

4/ "A Certificate Authority can issue you a digital certificate for code signing for a fee. "

This basically means that we have to pay money to some anonymous "trusted" authority to get our digital certificates... this starts to go into the realm of privacy. We all know that this is completely safe and that the rumours of back doors built into the encryption systems for international versions of US software is completely false... (<http://www.iptvreports.mcmail.com/ic2kreport.htm> , a must read if you are into security and privacy issues)

There's many more issues that can be delved into with MS's current approach to reduce (I cannot say "eliminate" because patching up a system that has a bad security model in the first place will never solve the problem) the problem with macro viruses.

If this system is "used properly", I believe that it will help reduce some of the problems with macro viruses, but I don't believe that it will work for long. Some bright spark will find yet another hole to take advantage of

and the system won't protect you.

The other flaw in this system is that there is an assumption that users will be educated enough to understand what all this means, certificates, trust, signing...yada yada yada. Not to knock the average user, but this will be a very very large vulnerability.

The real solution is to disable macros in MS Office software permanently with no way to turn it back on. You can actually do it in office 2000, as long as you are running Windows 2000 or NT4SP4 or greater.

(Do I hear another upgrade cycle spinning in here?)

Don't get me wrong, at the end of the day I am happy to use MS software in spite of the problems. I understand that the software is not secure. I keep my AV software updated. I learn about where a document comes from or I never enable the macros. If I keep the limitations in mind, I have no surprises or disappointments.

In fact, the last successful virus attack I have ever suffered was back in '92 when I received an infected floppy disk from someone I trusted to know better. He got me twice! Whoops...

Maybe I'm too paranoid..., yeah that's it.

Paul Walker, senior consultant, james martin + co
paul.walker AT jamesmartin.com

⚡ Embedded NT... in case you don't have enough to worry about

already

"Gregor Ronald" <gregor@caverock.net.nz>

Mon, 24 May 1999 20:25:00 +1200

Here's a harmless one, but it still shows that things don't always go right;

New Zealand's new national Museum, Te Papa, in Wellington, is a "modern" museum - highly interactive. I arrived as the doors opened, walked up to a touch-screen information kiosk, and it said "At least one device or service failed..... check the Event Log." Ah, I thought, this is the NT we all know so well! A touch on OK and it booted, so the load failure was something minor.

Now, if it had been a plane, or a ship, or a high-speed elevator, or.....

Gregor Ronald, Christchurch, New Zealand <http://www.caverock.net.nz/~gregor>

Home: gregor@caverock.net.nz Work: ronaldg@chchpoly.ac.nz

🔥 REVIEW: "Microsoft Windows NT 4.0 Security, Audit, and Control"

Rob Slade <rslade@sprint.ca>

Tue, 25 May 1999 10:10:25 -0800

BKWNTSAC.RVW 990409

"Microsoft Windows NT 4.0 Security, Audit, and Control", James G. Jumes et al, 1999, 1-57231-818-X, U\$49.99/C\$71.99/UK#45.99

%A James G. Jumes

%A Neil F. Cooper

%A Paula Chamoun
%A Todd M. Feinman
%C 1 Microsoft Way, Redmond, WA 98052-6399
%D 1999
%G 1-57231-818-X
%I Microsoft Press
%O U\$49.99/C\$71.99/UK#45.99 800-6777377 fax: 206-936-7329
%P 318 p.
%S Technical Reference
%T "Microsoft Windows NT 4.0 Security, Audit, and Control"

The primary audience described in the introduction seems to be security professionals. However, system administrators, technology managers, and CIOs are mentioned as well. The attempt at breadth of coverage usually does not bode well in works like these.

Chapter one discusses an information security model based upon the business (and other) objectives of the institution in question. While valid as far as it goes, and even possibly helpful when formulating security policy, this by no means provides a structure from which to view either security policy or procedures, let alone implement a complex set of controls. The widget company, beloved of management writers, is described in chapter two. For the purposes of assessing security in real world working environments, this particular widget company seems to be astoundingly simple and homogeneous.

Chapter three starts out talking reasonably about security policy, starts to get flaky in risk assessment (I would definitely worry about a .45 chance of an earthquake), and tails off into trivia. Monitoring, in chapter four, looks first at system performance and diagnostics, and then gets

into event logging without really going into the concepts. Many areas of physical security are left uncovered in chapter five. Chapter six discusses domains, trust relationships, and remote access permissions. Dialogue boxes for user accounts and groups are listed in chapter seven. There is some mention of the commonly "received wisdom" in regard to these topics, as there is in chapter eight regarding account policies, but nothing very significant. File system, share, and other resource control is covered in chapter nine. Chapter ten is a bit of a grab bag without much focus. The registry is reviewed in chapter eleven. Chapter twelve looks briefly at power supplies and backups. Although it talks about auditing, chapter thirteen is more of a checklist of security features to think about. Appendix A is a bit better in this regard: it lists recommended settings across a number of functions for six different types of systems.

There is some discussion of options as the various functions are addressed, so, in a sense, this is a start towards full coverage of NT security. It has a long way to go, though. In addition, the deliberation comes at the cost of a loss of some detail in terms of security implementation.

copyright Robert M. Slade, 1999 BKWNTSAC.RVW 990409
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

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



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 43

Friday 4 June 1999

Contents

- [A THAAD Day in Black Rock](#)
[PGN](#)
- [Ghost bridge](#)
[Meine van der Meulen](#)
- [Y2K Test Knocks Out Fiji's Telecommunications](#)
[Doneel Edelson](#)
- [Hackers take down FBI and Senate Internet sites ...](#)
[Keith A Rhodes](#)
- [Crackers do for gov't what critical infrastructure report couldn't](#)
[John Gilmore](#)
- [Errors in the Cox report on Chinese nuclear spying](#)
[PGN](#)
- [Hoax takes down country's phone networks](#)
[Lloyd Wood](#)
- [Symbols silently slip south: it's not Greek to pdf](#)
[Bryan O'Sullivan](#)
- [John Denver and interfaces](#)
[Lindsay Marshall](#)
- [Smart Identity Card to debut in Malaysia](#)
[Anonymous](#)

- [Late-night movie viewing and computerized ticket sales](#)
[Steve Fenwick](#)
 - [Senator Hatch - Trademark](#)
[Alan Barclay](#)
 - [BUGTRAQ may be banned in Australia](#)
[Peter Jeremy via Seth David Schoen](#)
 - [Re: Microsoft "fixes" the MS Office ... vulnerability](#)
[David Mediavilla](#)
 - [We don't care, we don't have to, we're the phone company!](#)
[John Pettitt](#)
 - [Firewall risks](#)
[Robert David Graham](#)
 - [Re: Allaire defects are nobody's fault?](#)
[Adam Shostack](#)
 - [A Problem with Biometrics](#)
[Andrew J Klossner](#)
 - [Re: Biometric risks](#)
[Ron Ruble](#)
 - [California will sell confidential wage data](#)
[PGN](#)
 - [Privacy Digests](#)
[PGN](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ A THAAD Day in Black Rock

"Peter G. Neumann" <neumann@csl.sri.com>
Wed, 26 May 99 11:22:54 PDT

The Pentagon halted a test of the Theater High-Altitude Area Defense (THAAD) missile-defense system, when a Hera target rocket malfunctioned. THAAD is under scrutiny after seven consecutive failed tests. [Source: Reuters item,

26 May 1999, seen in the *San Francisco Chronicle*.]

[Maybe this renewed attempt to develop the Star Wars technology should be left to George Lukas, who seems to do it much better. Perhaps animating the system without ever building it would be the most cost-effective strategy. PGN]

Ghost bridge

Meine van der Meulen <M.van.der.Meulen@simtech.nl>

Wed, 2 Jun 1999 16:32:10 +0200

Kropswolde, Monday. The bridge on the Meerweg in the village Kropswolde manifested itself as a ghost bridge during the weekend. A car driver was trapped when he passed the bridge and both barriers suddenly closed. The police managed to rescue the man. Just after this rescue action, the bridge suddenly opened and closed without apparent reason. The village closed the bridge. [Source: *Algemeen Dagblad*, 1 Jun 1999]

M.J.P. van der Meulen <meine.van.der.meulen@simtech.nl>

Y2K Test Knocks Out Fiji's Telecommunications

"Edelson, Doneel" <doneeledelson@aciins.com>

Wed, 26 May 1999 13:13:43 -0400

Fiji's telecommunications services were completely shut down for several hours on 24 May 1999 when a Y2K test by Telecom Fiji Ltd. caused the entire system to crash. [See <http://www.tfl.com.fj/>. Source: Yahoo Asia News - Technology, Newsbytes item by Adam Creed, Post-Newsweek Business Information, Inc., 24 May 1999: PGN-ed.]

⚡ Hackers take down FBI and Senate Internet sites ...

"Keith A Rhodes" <rhodesk.aimd@gao.gov>
Fri, 28 May 1999 13:13:37 -0500

Both FBI and Senate Web sites were attacked on 27 May 1999, evidently in retaliation for the FBI's harassment of certain hacker groups -- including one that apparently cracked the White House site earlier this month (for which Eric Burns (Zyklon) was indicted. Both sites were removed from service, although only the Senate site was penetrated and altered. [Source: Associated Press item by Ted Bridis, 28 May 1999; PGN-ed.]

[The Department of Interior and a Govt facility at Idaho Falls were also hit on 31 May 1999. Other attacks were reported subsequently. PGN]

⚡ Crackers do for gov't what critical infrastructure report couldn't

John Gilmore <gnu@toad.com>
Thu, 03 Jun 1999 19:05:50 -0700

"There's a government-wide effort to make sure that our computer systems remain secure," White House Press Secretary Joe Lockhart said in a briefing.

<http://www.zdnet.com/zdnn/stories/news/0,4586,2268574,00.html>

As usual, the computer underground is doing a service to the country by making it clear just how shallow the government's understanding of computer security is. They are quite curiously refraining from damaging anything in their intrusions but the egos of the bureaucracies involved. As usual, the first response of the Feds is to threaten dire punishment for the messengers. But they are being prodded into actually attempting to keep serious attackers out, a novel idea somewhat overdue for consideration.

Perhaps this is heresy, but has the computer underground considered demonstrating that it can break into electrical power distribution computers, and the phone network, so those will get secured too?

John

✶ Errors in the Cox report on Chinese nuclear spying

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

Fri, 4 Jun 1999 16:35:12 PDT

An article by James Oberg on the ABC News Science website documents

many misstatements in the Cox report.

<http://www.abcnews.go.com/sections/science/DailyNews/oberg990602.html>

✶ Hoax takes down country's phone networks

Lloyd Wood <L.Wood@surrey.ac.uk>

Tue, 11 May 1999 00:16:27 +0100 (BST)

http://news.bbc.co.uk/hi/english/world/middle_east/newsid_340000/340104.stm

Article claiming:

1. Lebanese radio station broadcasts hoax claiming cellular networks are affected by Chernobyl virus (the current popular student excuse for tardy wordprocessed reports, if my experience is at all typical).
2. Lebanese immediately stop using popular cellular networks, and switch to landline networks to warn each other of anticipated cellular problems. (Israel's also known for its heavy cellular use.)
3. Landline networks are promptly overloaded due to normally-large and now-displaced cellular use and warnings of problems. The radio broadcast has prompted a flash crowd and service outages result.
4. Conspiracy theorists suspect underlying motives in finger-pointing wake, while ignoring the risks of behaving rationally when

armed

with false information and not having meme countermeasures in place.

Handling and selectively discarding the majority of calls from flash crowds caused by e.g. television phone-ins is trivial; it's arranged in advance (if the media people know their jobs...) and you know where the flash calls are going. But how do you effectively deal with a many-to-many surge like this?

Dimensioning telco switch capacity for expected use doesn't lead to graceful degradation under heavy load, but hey, that's Erlang for you.

Legacy local loop is the real constraint/problem; degrading the quality of digitised voice traffic in the pleisynchronous backbone and restoring at the other end to increase capacity is a trivial codec application, and just a minor step up from silence suppression.

I think this is something like the sinister inverse of the oft-cited disaster scenario, where network damage is suffered and any remaining functional cellular and landline capacity would be immediately overwhelmed by people trying to locate loved ones. The callers are behaving rationally and selfishly; the networks can't cope effectively. I'd say 'tragedy of the commons' if it wasn't for the fact you pay for phone service.

This is far more impressive than that "if someone tells you to dial #91, don't" meme, which got through multiple countries to users of all types of mobile networks recently. But the "withdraw money from banks for Y2K to

avoid the financial crash the withdrawals contribute to" and the "don't purchase Iridium handsets because Iridium are in trouble" memes may yet have far more impressive results as self-fulfilling prophecies.

<L.Wood@surrey.ac.uk>PGP<<http://www.ee.surrey.ac.uk/Personal/L.Wood/>>

🔥 Symbols silently slip south: it's not Greek to pdf

"Bryan O'Sullivan" <bos@serpentine.com>
Wed, 2 Jun 1999 20:00:07 -0700 (PDT)

In the course of some exploratory work I am doing, I recently downloaded a technical paper in Adobe's Portable Document Format:

<http://research.microsoft.com/copyright/accept.asp?path=http://research.microsoft.com/~hoppe/siggraph96pm.pdf&pub=acm>

After a brief perusal of the abstract using Adobe's free Acrobat Reader for Linux, I decided that the paper was interesting enough to print out, and squirreled the hardcopy away for later perusal.

When I went to read the paper today, I was a little surprised to find that it had not reproduced very well. In particular, much of the mathematical notation in the paper was garbled or missing; Greek characters and curly braces were notable by their absence. All of this information was represented correctly on-screen by Acrobat Reader; it was silently mangled when I printed the document out.

Worried, I did a little more experimentation. The free gv viewer had no trouble displaying the paper on my screen (but I didn't try printing it out). The free xpdf viewer dropped most of the mathematical notation, but the author at least documented this shortcoming (relating to embedded fonts).

As I am not near a printer at the moment, I am going through my hardcopy of the paper with a pen, adding the missing characters. Most disturbingly of all, as I began to make these corrections, I found that the mathematical symbol for inequality (an "equals" symbol with a slash through it) was misrendered on paper as that for equality.

The RISK seems clear - technical papers presented for downloading in PDF can be arbitrarily garbled by viewers in ways that may be difficult to spot.

✶ John Denver and interfaces

<Lindsay.Marshall@newcastle.ac.uk>
Tue, 1 Jun 1999 13:55:50 +0100 (GMT)

<<http://www.asktog.com/columns/027InterfacesThatKill.html>>
describes
how John Denver was killed because of a modified interface in
the plane
he was flying.

<http://catless.ncl.ac.uk/Lindsay>

[The builder had changed the designer's plans, placing the fuel-tank selector controls rather weirdly over the pilot's shoulder, unlabelled, with up for off, down for the right tank, and to the right for the left tank. There are more curiosities in the NTSB report, at www.nts.gov. PGN]

Smart Identity Card to debut in Malaysia

<[Identity anonymized]>

Tue, 1 Jun 1999 09:29:15 +0100 (BST)

Malaysia's compulsory National Registration Identity Card (NRIC), required for doing anything official or semi-official (such as banking, buying a car, etc) is to become SMART and include financial and health data, driving and travel rights and criminal offences in addition to the residence address and thumbprints on the current laminated paper version.

The thumbprint, currently underused, is set to become the standard computerised ID biometric used by government agencies.

The new NRIC may also become the national payment system.

NRIC numbers are issued at birth (on the birth certificate) but the card itself is issued at the age of 12, and must thereafter be carried at all times.

I have no information about the private company that has won the

contract to supply the new smart cards. Nor have I heard of any public scrutiny mechanism to ensure that the technology does not contain flaws that will enable this data to fall into the wrong hands.

[Source: article by Philip Golingai, Your smart IC Card with personal data of holder expected out in August next year, The Star, 1 Jun 1999.]

🔥 Late-night movie viewing and computerized ticket sales

Steve Fenwick <scf@w0x0f.com>
Thu, 20 May 1999 19:43:20 -0700

If you're an after-midnight movie-goer, check your tickets!

I bought tickets last weekend for "Phantom Menace", dated Wednesday, May 19th, 12:15AM. Bright RISKS readers can guess what's coming next...

The theatre's computer apparently does not recognize midnight as the break between two days, it uses the normal box office opening time (11AM) as the break. So their 12:15AM 5/19 show was really on 5/20 at 12:15AM.

Oops.

So I wound up seeing the show on 5/18 (according to their computer), a full day before the movie officially opened. Take **that**, Darth Vader!

Steve Fenwick <scf@w0x0f.com> <http://www.w0x0f.com>

[Star Warps? PGN]

✶ Senator Hatch - Trademark

Alan Barclay <gorilla@elaine.drink.com>

Thu, 27 May 1999 12:55:40 -0400

ABC News apparently thinks that Senator Orin Hatch has registered his name as a trademark, in

<http://www.abcnews.go.com/sections/tech/DailyNews/netbombs990525.html>

"The amendment, sponsored by Sens. Orrin Hatch [*R*] of Utah and Dianne Feinstein (D) of California, does not make it illegal to simply provide the information, However."

Here "[*R*]" designates the \256 code that prints as the circle-R registered-trademark symbol. Obviously we're seeing some sort of translation between (R) and the circle-R, even though in this case the

(R) is the correct text. An old story of over-enthusiastic substitution.

[By the time I checked it out the next day, it had been fixed. PGN]

✶ BUGTRAQ may be banned in Australia

Peter Jeremy <peter.jeremy@AUSS2.ALCATEL.COM.AU>

Thu, 27 May 1999 08:21:26 +1000

To: BUGTRAQ@netspace.org

[Forwarded to RISKS by Seth David Schoen <schoen@loyalty.org>. PGN]

This message is intended as a call-to-arms for BUGTRAQ subscribers as well as a warning to subscribers in other countries.

Yesterday, the Australian Senate (Upper House of the Federal Government) passed legislation to censor the Internet (I don't have a URL for the final legislation at present). This legislation mandates the censorship of Internet content (which includes mailing lists) as if it was a film. All Australian ISPs are required filter overseas content that would be rated X or RC under the Australian classification guidelines (see <http://www.oflc.gov.au/PDFs/Film%20&%20Video%20Guidelines.pdf>).

The RC (Refused Classification) category states:

"The Classification Code sets out the criteria for refusing to classify a film or video. The criteria fall into three categories. These include films that: ... promote, incite or instruct in matters of crime or violence."

and later

"Films and videos will be refused classification: or if they contain: ... detailed instruction in: matters of crime or violence,"

BUGTRAQ is a full-disclosure list and regularly contains detailed descriptions of how to break into computers. Breaking into computers is a crime in Australia. It is therefore possible that BUGTRAQ could be classified "RC" and hence banned in Australian.

Refer to <http://www.efa.org.au/> for further information.

Peter Jeremy (VK2PJ)

peter.jeremy@alcatel.com.

au

Alcatel Australia Limited

41 Mandible St

Phone: +61 2 9690 5019

ALEXANDRIA NSW 2015

Fax: +61 2 9690 5982

----- End forwarded message -----

Seth David Schoen <schoen@loyalty.org>

<http://ishmael.geecs.org/~sigma/> (personal) <http://www.loyalty.org/> (CAF)

[Ah, yes, and Linux source code contains some dirty words.
PGN]

⚡ Re: Microsoft "fixes" the MS Office ... vulnerability ([R 20 42](#))

Mediavilla David <davidme.Forum@BigFootNOSPAM.com>

Thu, 27 May 1999 14:59:53 +0200

After reading [RISKS 20.42](#), it came to my mind a combination of risks. Paul Walker mentioned the Microsoft plan to sign Office 2000 macros. In "German government criticizes own style in Word documents", Debora Weber-Wulff mentions that Office automatically fills author and organization information from the current machine.

I am not sure if this means Microsoft may have enabled that every macro that came to my system without signing, say an Office 97 virus that I inadvertently loaded, will come out as signed by me. Then, everybody who trusts me will become infected (and I will be blamed).

I asked Paul Walker (the original poster to RISKS). According to

the MS document, with security settings as 'high' unsigned macros are silently disabled. Set to 'low', Office 2000 will silently run them. Set to 'medium', Office 2000 will ask the user.

<PAUL WALKER>

Reading the document further does not explicitly state what happens to the macro when it is opened under low security settings. It would appear that the macro will run, but it will not be signed. Signing a macro appears to be something that you have to do yourself.

It would appear that this won't be a danger, but...

Can you have an untrusted vb code make a function call that would sign the macro? In current versions of word, almost every menu function (maybe all, I have not checked) can be done through the vb macros. Until I get a copy of the software in my hands, I won't be able to confirm this...
</PAUL WALKER>

David Mediavilla Ezquibela <davidme.forum@bigfootNOSPAM.com>
[ES/EN/EO/EU] (Lan)

⚡ We don't care, we don't have to, we're the phone company!

John Pettitt <jpp@cloudview.com>
Tue, 25 May 1999 16:47:14 -0700

I recently made a couple of trips to the UK on business and not wishing to spend the entire US GDP on phone bills (UK hotels phones should be avoided

at all costs) I used my MCI card to call home and check e-mail.

When I got back my MCI bill was full of "operator assisted" calls from the UK to the US (billed at more than \$2 per min). I called MCI and after they dialed the number and confirmed that it was indeed a modem and that no their operators could not speak V.90 I got a credit for \$200 or so.

My next MCI bill was for \$4000+ - with exactly the same problem (in this case close to \$3000 in over billing). This time they would not issue a credit (they can't tell me why - I'm not allowed to talk to the people who decide these things).

There are a whole bunch of risks here:

- 1) Systems that are wrongly configured and over bill even when used according to the instructions (and still do it a month after first reported)
- 2) Customer service systems that prevent customers from talking to decisionmakers.
- 3) No exception system to allow issues to be escalated.

I'm reminded of the well know phrase "We don't care, we don't have to, we're the phone company".

John Pettitt (ex MCI customer, about to hand the whole mess to the lawyers)

Allaire firewall RISKS

"Robert David Graham" <rob-risks@netice.com>

Tue, 1 Jun 1999 19:49:15 -0700

In the past couple months, hundreds (if not thousands) of web sites using Allaire's ColdFusion have been hacked (their web pages have been defaced).

When interviewed by the press, one site administrator said, "We are installing a firewall so that this won't happen again".

However, firewalls do not protect against this particular hack.

Explanation: Firewall technology is based on "port filters". The average web server has many ports open for a variety of reasons, but needs only port 80 in order to serve web pages. However, ColdFusion runs as part of the web server reachable at port 80. QED, placing a firewall in front of web server provides no protection against the ColdFusion hack.

Firewalls do not "prevent" hacks, as most people believe. They simply reduce RISKS by reducing the number of ports or IP addresses that may be exposed inadvertently on the Internet. The remaining ports (such as e-mail, web, and FTP servers) can often be hacked.

In practice, firewalls probably increase RISKS overall. Consider a study of Berlin taxi drivers who were given anti-lock breaks: the taxi drivers started driving more aggressively, and had more accidents. Therefore, the study concluded that anti-lock actually INCREASES RISKS. What is really going on is that firewalls/ABS only decrease RISKS if behavior is left unchanged, but the added security encourages RISKY behavior.

The ColdFusion bug was not really Allaire's fault -- the bug was in a sample script that Allaire recommends be removed from a production web server.

Almost every web-site creation package like ColdFusion has the same problem, including Microsoft's ASP scripting, FrontPage web hosting, and sample CGI programs. Administrators feel safe behind firewalls and do not diligently check their web servers for these problems. For the most part, crackers who intend to deface web pages or steal credit card information from web servers do not care about firewalls that might protect the target servers.

Robert Graham

<http://www.networkice.com/advice>

✉ Re: Allaire defects are nobody's fault? (Graham, [RISKS-20.43](#))

Adam Shostack <adam@homeport.org>

Thu, 3 Jun 1999 12:31:20 -0400

Robert David Graham wrote:

| The ColdFusion bug was not really Allaire's fault -- the bug was in a
| sample script that Allaire recommends be removed from a production web
| server. Almost every web-site creation package like ColdFusion has the
| same problem, including Microsoft's ASP scripting, FrontPage web
| hosting, and sample CGI programs. Administrators feel safe behind

I'm sorry, but that's not the case. The ColdFusion bug was Allaire's fault.

They wrote and shipped crap sample code that has security flaws in it. That code has probably been modified into other vulnerable programs. There are a reasonably large number of secure programming FAQs available; Matt Bishop has one, there's one in Garfinkel and Spafford, there's one I wrote.

I've seen academic references in 1976 or so that programs that don't validate their input are vulnerable to attack. To absolve a company of blame for shipping bogus code is wrong. They screwed up. They got lots of people in trouble. They wasted lots of people's time.

If you don't have time to do the sample code right, don't ship it. It's been a long time since a problem like this was found in Apache; NCSA had a slew, and the web folks learned. You can read the history of it in the bugtraq archives.

⚡ A Problem with Biometrics

Andrew J Klossner <andrew@pogo.WV.TEK.COM>
Thu, 27 May 1999 13:37:07 -0700

Unlike account numbers and PINs, biometrics suffer from the Universal Identifier problem. I can use a different account number and password at each of several institutions, and can change them at need. Switching to iris scan would have me use the same immutable password

everywhere.

This will also lead to unwanted pooling of data by commercial and government interests. Dig out any article on the evils of the U.S. Social Security Number as identifier and change "SSN" to "iris scan" throughout.

-- Andrew Klossner (andrew@pogo.wv.tek.com)

✶ Re: Biometric risks

Ron Ruble <raffles1@worldnet.att.net>

Mon, 24 May 1999 05:33:33 -0400

In [RISKS-20.41](#), Dan Wallach and Paul Lewis Gittins both mentioned risks involving lack of an alternative to biometric identification. They identified the risk of not servicing visually impaired individuals whose irises can't be scanned.

In the US, failure to provide a fallback method of identification may well place the owners of the system at legal risk.

Not having a fallback may well be considered a violation of the Americans With Disabilities Act. The ADA does not spell out specific rules or requirements, but does make the statement that 'reasonable accommodation' must be made for all persons with disabilities. It would be up to the jury to decide whether having a card and PIN as a fallback for the biometric system was reasonable.

Some might argue that many visually impaired people would go to the human tellers anyway, and during banking hours, this may be an acceptable accommodation. But it does not provide the 24-hour availability of the ATM.

In addition, the manufacturers of the devices may be at risk if they install or recommend installing the devices without fallback options.

I seem to recall that several European nations have similar laws that require similar accommodations for the disabled. I hope some of the Europeans who frequent this forum will comment on that.

Ron Ruble, Raffles Software Development, Inc.

California will sell confidential wage data

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

Fri, 4 Jun 1999 16:33:19 PDT

California will begin selling confidential wage data of 14 million of its residents to private information companies, car dealers and creditors wanting to check an individual's annual income. [...] No data would be shared without the written permission of the individual, state officials said. However, private companies that are deemed qualified to access the data would operate on an honor system and would not be required to show proof of each individual's written permission before accessing

the
information. [Do you believe this one? See nandotimes, 3 Jun
1999,
<http://www.nandotimes.com/noframes/story/0,2107,55865-89293-634754-0,00.html>]

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:

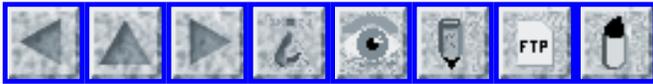
<http://www.vortex.com>

* 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 20: Issue 44

Tuesday 15 June 1999

Contents

- [GPS kills 8 in air](#)
[Lloyd Wood](#)
- [W32/ExploreZip.worm "virus" and user interfaces](#)
[Steven M. Bellovin](#)
- [CERT Advisory CA-99.06 - New information regarding ExploreZip](#)
[CERT](#)
- [Downloading Y2K fixes to Internet Explorer leads to clock problem](#)
[Paul Karger](#)
- [ActiveX Security Revisited](#)
[Steve Loughran](#)
- [Unwanted wildcard match](#)
[Nick Brown](#)
- [Bank sued over client data sale](#)
[Monty Solomon](#)
- [UAL -- the UnFriendly Cybersky?](#)
[David Lesher](#)
- [Info on RISKS \(comp.risks\)](#)

GPS kills 8 in air

Lloyd Wood <L.Wood@surrey.ac.uk>
Mon, 7 Jun 1999 15:46:47 +0100 (BST)

[...] 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.

<L.Wood@surrey.ac.uk>PGP<<http://www.ee.surrey.ac.uk/Personal/L.Wood/>>

[Quite old, but not previously covered. PGN]

⚡ W32/ExploreZip.worm "virus" and user interfaces

"Steven M. Bellovin" <smb@research.att.com>

Fri, 11 Jun 1999 13:26:33 -0400

Subtitle: "I got it from Agnes, she got it from Jim"... (Tom Lehrer)

Another month, another killer "virus". By now, everyone has heard about this latest piece of malware. But what's interesting is that part of the way it spread appears to be dependent on the user interface.

The actual damage was done by an executable, a .EXE file. However, according to some reports the file itself contained the icon of a .ZIP file. Thus, even moderately cautious users could be tricked into opening the file -- which in this case meant executing it.

The underlying problem is that there are two different mechanisms used to determine file type, and hence how it should be "opened". One is what is displayed to the user; the other is what is actually used. That way lies danger.

[But it can also spread worm-like without your help. Some folks still need to learn some of the lessons from the 1965 efforts on Multics!

See

<http://www.multicians.org/>

PGN]

⚡ CERT Advisory CA-99.06 - New information regarding ExploreZip

CERT Advisory <cert-advisory@cert.org>

Mon, 14 Jun 1999 07:16:05 -0400

CERT Advisory CA-99-06-explorezip

Original issue date: Thursday June 10, 1999

Last Revised Date: June 14, 1999

Added information about the program's self-propagation via networked shares; also updated anti-virus vendor URLs.

Source: CERT/CC

Note: The CERT Coordination Center has discovered new information regarding the ExploreZip worm. This re-issue of CERT Advisory CA-99-06 contains new information regarding an additional means by which the Worm can spread, and a caution about disinfecting your systems. We will continue to update this advisory as new information is discovered. We encourage you to check our web site frequently for any new information.

Systems Affected

- * Machines running Windows 95, Windows 98, or Windows NT.
- * Machines with filesystems and/or shares that are writable by a user of an infected system.
- * Any mail handling system could experience performance problems or a denial of service as a result of the propagation of this Trojan horse program.

Overview

The CERT Coordination Center continues to receive reports and inquiries regarding various forms of malicious executable files that are propagated as file attachments in electronic mail.

During the second week of June 1999, the CERT/CC began receiving reports of sites affected by ExploreZip, a Trojan horse/worm program that affects Windows systems and has propagated in e-mail attachments. The number and variety of reports we have received indicate that this has the potential to be a widespread attack affecting a variety of sites.

I. Description

Our original analysis indicated that the ExploreZip program is a Trojan horse, since it initially requires a victim to open or run an e-mail attachment in order for the program to install a copy of itself and enable further propagation. Further analysis has shown that, once installed, the program may also behave as a worm, and it may be able to propagate itself, without any human interaction, to other networked

machines that have certain writable shares.

The ExploreZip Trojan horse has been propagated between users in the form of e-mail messages containing an attached file named zipped_files.exe. Some e-mail programs may display this attachment with a "WinZip" icon. The body of the e-mail message usually appears to

come from a known e-mail correspondent, and typically contains the following text:

I received your email and I shall send you a reply ASAP.

Till then, take a look at the attached zipped docs.

The subject line of the message may not be predictable and may appear to be sent in reply to previous e-mail.

Opening the zipped_files.exe file causes the program to execute. It is possible under some mailer configurations that a user might automatically open a malicious file received in the form of an e-mail attachment. When the program is run, an error message is displayed:

Cannot open file: it does not appear to be a valid archive. If this file is part of a ZIP format backup set, insert the last disk of the backup set and try again. Please press F1 for help.

Destruction of files

- * The program searches local and networked drives (drive letters C through Z) for specific file types and attempts to erase the contents of the files, leaving a zero byte file. The targets may include Microsoft Office files, such as .doc, .xls, and .ppt, and various source code files, such as .c, .cpp, .h, and .asm.
- * The program may also be able to delete files that are writable to it via SMB/CIFS file sharing. The program appears to look through the network neighborhood and delete any files that are shared and writable, even if those shares are not mapped to networked drives on the infected computer.
- * The program appears to continually delete the contents of targeted files on any mapped networked drives. The program does not appear to delete files with the "hidden" or "system" attribute, regardless of their extension.

System modifications

- * The zipped_files.exe program creates a copy of itself in a file called explore.exe in the following location(s):

On Windows 98 - C:\WINDOWS\SYSTEM\Explore.exe

On Windows NT - C:\WINNT\System32\Explore.exe

This explore.exe file is an identical copy of the zipped_files.exe Trojan horse, and the file size is 210432 bytes.

MD5 (Explore.exe) = 0e10993050e5ed199e90f7372259e44b

- * On Windows 98 systems, the zipped_files.exe program creates an entry in the WIN.INI file:

```
run=C:\WINDOWS\SYSTEM\Explore.exe
```

On Windows NT systems, an entry is made in the system registry:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows
  NT\CurrentVersion\Windows]
  run = "C:\WINNT\System32\Explore.exe"
```

Propagation via file sharing

Once explore.exe is running, it takes the following steps to propagate to other systems via file sharing:

- * Each time the program is executed, the program will search the network for all shares that contain a WIN.INI file with a valid "[windows]" section in the file.
- * For each such share that it finds, the program will attempt to
 - + copy itself to a file named _setup.exe on that share
 - + modify the WIN.INI file on that share by adding the entry "run=_setup.exe"

The account running the program on the original infected machine needs to have permission to write to the second victim's shared directory. (That is, no vulnerabilities are being exploited in order for the program to spread in this manner.)

The _setup.exe file is identical to the zipped_files.exe and explore.exe files on the original infected machine.

- * The original infected system will continue to scan shares that have been mapped to a local drive letter containing a valid WIN.INI file. For each such share that is found, the program will "re-infect" the victim system as described above.

On Windows 98 systems that have a "run=_setup.exe" entry in the WIN.INI file (as described previously), the C:\WINDOWS_setup.exe program is executed automatically whenever a user logs in. On Windows NT systems, a "run=_setup.exe" entry in the WIN.INI file does not appear to cause the program to be executed automatically.

When run as _setup.exe, the program will attempt to

- * make another copy of itself in C:\WINDOWS\SYSTEM\Explore.exe

- * modify the WIN.INI file again by replacing the "run=_setup.exe" entry with "run=C:\WINDOWS\SYSTEM\Explore.exe"

Note that when the program is run as _setup.exe, it configures the system to later run as explore.exe. But when run as explore.exe, it attempts to infect shares with valid WIN.INI files by configuring those files to run _setup.exe. Since this infection process includes local shares, affected systems may exhibit a "ping pong" behavior in which the infected host alternates between the two states.

Propagation via e-mail

The program propagates by replying to any new e-mail that is received by the infected computer. The reply messages are similar to the original e-mail described above, each containing another copy of the zipped_files.exe attachment.

We will continue to update this advisory with more specific information as we are able to confirm details. Please check the CERT/CC web site for the current version containing a complete revision history.

II. Impact

- * Users who execute the zipped_files.exe Trojan horse will infect the host system, potentially causing targeted files to be destroyed.
- * Users who execute the Trojan horse may also infect other networked systems that have writable shares.
- * Because of the large amount of network traffic generated by infected machines, network performance may suffer.
- * Indirectly, this Trojan horse could cause a denial of service on mail servers. Several large sites have reported performance problems with their mail servers as a result of the propagation of this Trojan horse.

III. Solution

Use virus scanners

While many anti-virus products are able to detect and remove the executables locally, because of the continuous re-infection process, simply removing all copies of the program from an infected system may leave your system open to re-infection at a later time, perhaps immediately. To prevent re-infection, you must not serve any shares containing a WIN.INI file to any potentially infected machines. If you share files with everyone in your domain, then you must disable shares with WIN.INI files until every machine on your network has been

disinfected.

In order to detect and clean current viruses, you must keep your scanning tools up to date with the latest definition files. Please see the following anti-virus vendor resources for more information about the characteristics and removal techniques for the malicious file known as ExploreZip.

Aladdin Knowledge Systems, Inc.

<http://www.esafe.com/vcenter/explore.html>

Central Command

<http://www.avp.com/zippedfiles/zippedfiles.html>

Command Software Systems, Inc

<http://www.commandcom.com/html/virus/explorezip.html>

Computer Associates

<http://www.cai.com/virusinfo/virusalert.htm>

Data Fellows

<http://www.datafellows.com/news/pr/eng/19990610.htm>

McAfee, Inc. (a Network Associates company)

<http://www.mcafee.com/viruses/explorezip/default.asp>

Network Associates Incorporated

<http://www.avertlabs.com/public/datafiles/valerts/vinfo/va10185.asp>

Sophos, Incorporated

<http://www.sophos.com/downloads/ide/index.html#explorez>

Symantec

<http://www.symantec.com/avcenter/venc/data/worm.explore.zip.htm>

1

Trend Micro Incorporated

<http://www.antivirus.com/vinfo/alerts.htm>

Additional sources of virus information are listed at

http://www.cert.org/other_sources/viruses.html

Additional suggestions

- * Blocking Netbios traffic at your network border may help prevent propagation via shares from outside your network perimeter.
- * Disable file serving on workstations. You will not be able to share your files with other computers, but you will be able to browse and get files from servers. This will prevent your workstation from being infected via file sharing propagation.
- * Maintain a regular, off-line, backup cycle.

General protection from e-mail Trojan horses and viruses

Some previous examples of malicious files known to have propagated through electronic mail include

- * False upgrade to Internet Explorer - discussed in CA-99-02
<http://www.cert.org/advisories/CA-99-02-Trojan-Horses.html>
- * Melissa macro virus - discussed in CA-99-04
<http://www.cert.org/advisories/CA-99-04-Melissa-Macro-Virus.html>
- * Happy99.exe Trojan Horse - discussed in IN-99-02
http://www.cert.org/incident_notes/IN-99-02.html
- * CIH/Chernobyl virus - discussed in IN-99-03
http://www.cert.org/incident_notes/IN-99-03.html

In each of the above cases, the effects of the malicious file are activated only when the file in question is executed. Social engineering is typically employed to trick a recipient into executing the malicious file. Some of the social engineering techniques we have seen used include

- * Making false claims that a file attachment contains a software patch or update
- * Implying or using entertaining content to entice a user into executing a malicious file
- * Using e-mail delivery techniques which cause the message to appear to have come from a familiar or trusted source
- * Packaging malicious files in deceptively familiar ways (e.g., use of familiar but deceptive program icons or file names)

The best advice with regard to malicious files is to avoid executing them in the first place. CERT advisory CA-99-02 discusses Trojan horses and offers suggestions to avoid them (please see Section V).

<http://www.cert.org/advisories/CA-99-02-Trojan-Horses.html>

This document is available from:

<http://www.cert.org/advisories/CA-99-06-explorezip.html>.

E-mail: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890 U.S.A.

CERT personnel answer the hotline 08:00-20:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by e-mail. Our public PGP key is available from http://www.cert.org/CERT_PGP.key. If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site <http://www.cert.org/>.

To be added to our mailing list for advisories and bulletins, send e-mail to cert-advisory-request@cert.org and include SUBSCRIBE your-e-mail-address in the subject of your message.

Copyright 1999 Carnegie Mellon University.
Conditions for use, disclaimers, and sponsorship information can be found in http://www.cert.org/legal_stuff.html.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office

NO WARRANTY

Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Revision History

June 10, 1999: Initial release
June 11, 1999: Added information about the appearance of the attached file
Added information from Aladdin Knowledge Systems, Inc.
June 14, 1999: Added information about the program's self-propagation via
networked shares; also updated anti-virus vendor URLs

[(S)lightly edited for RISKS. PGN]

⚡ Downloading Y2K fixes to Internet Explorer leads to clock problem

Paul Karger <karger@watson.ibm.com>

Wed, 09 Jun 1999 15:54:47 -0400

I was attempting to install service pack 2 of Internet Explorer 4.01 in order to meet corporate Y2K requirements and ran into the following interesting problem.

To install service pack 2, you first download a small program from Microsoft. You run that program, and after asking you some questions, it then downloads the full service pack 2. One of the questions was whether you wanted to install the service pack or just download the files. I replied that I just wanted to download the files. My intention was to virus check them, before actually performing the install.

However, when it attempted to download the full service pack, the small downloader complained that my system clock was not set correctly, and that therefore it could not perform the download. I checked, and my system clock was set correctly. Pushing the help button on the error screen gave information about setting the clock, followed by a somewhat cryptic comment about security settings in Internet Explorer.

My already installed version Internet Explorer was set to high security for all zones, as the dangers of ActiveX, Java, and Javascript are well known.

As an experiment, I lowered the security setting for the Internet zone to medium, and the download proceeded without error. Note that ostensibly, I was only downloading files, not running anything, yet the security protection level had to be lowered, not to mention the bogus error message.

I then raised the setting back to high, performed the virus check, and then tried to install the downloaded files. Again it complained about the clock setting, and again I had to lower the security setting to medium to permit the install to proceed. (This time, I was actually executing code, so I suppose the lowered setting was appropriate, but it still complained about the clock, rather than the security setting.)

I suppose that downloading any code (even if not executing it) from the Microsoft web site could be considered a security risk and therefore not compatible with "high security". However, I don't think that was Microsoft's intention, and surely it should not have been reported as a clock setting problem.

(Footnote for technical accuracy: In the above description, I said that I used the high security setting in Internet Explorer. This was artistic license on my part. Actually, I used the custom setting to get an even more conservative setting than what Microsoft calls "high security". "High security" still allows certain kinds of "safe" scripts to run, and I prefer to disable even "safe" scripts. However, the bogus error occurred not just on the custom very high setting, but also on Microsoft's own high security setting.)

(To be fair to Microsoft, a full viral scan of both the downloaded service pack and of the system after the service pack was installed revealed no problems, nor did I seriously expect any. However, I routinely virus scan any and all downloaded files, regardless of their source.)

Paul

⚡ ActiveX Security Revisited

"Steve Loughran" <slo99@iseran.com>

Wed, 9 Jun 1999 12:22:00 +0100

The latest Microsoft security bulletin

<http://www.microsoft.com/security/bulletins/ms99-018.asp>) includes two Internet Explorer patches. The first is a classic stack overrun -a web page

can supply an icon for use when adding to the favourite links list, and a malformed icon could overrun the stack and so execute arbitrary code.

The second fault is a security hole in ActiveX control, and is a simple instantiation of the problem covered in [RISKS-18.85](#) and [RISKS-18.86](#), namely than code signing is a far less safe method of software distribution

than a 'sandbox' for untrusted code.

It so happens that one of the ActiveX controls dating from IE3 can be used

to test for the presence or absence of files on a hard disk, and while no access to the contents is granted, it can be used to build up a picture of

what applications are installed. My demonstration page

<http://www.iseran.com/ActiveX/filesearch.html>) shows a naive script looking for common windows files in well known places -it could just as easily look for well known applications as a preamble to an application specific attack.

The insecure 'Preloader' control has some interesting properties.

Firstly,

it is signed by Microsoft, showing that even the inventors of ActiveX and the entire Win32 API did not test their controls rigorously enough.

Secondly, some distributions of Internet Explorer may have automatically installed the control, in which case the control download or signature verification process is bypassed.

It so happens that the default security settings of the Outlook and Outlook

Express e-mail messages, which means anyone could send a web page referencing the control to any known recipient and stand a moderate chance

of being able to enumerate some disk files, possibly with no visible notification to the recipient. This strikes me as a more serious problem than the risk incurred by looking at random web pages, as it enables attacks

targeted at individual recipients.

Within four weeks of notifying Microsoft via their security e-mail alias the company announced the problem, and withdrew the control from their own web site, which seems a reasonable response time. Of course, if ActiveX had included a mechanism whereby the signer of a control could retroactively revoke that control then it would have been trivial to disable the control remotely. Instead the company had to patch IE to permanently disable the control. Few other companies would have this luxury.

While enabling or disabling ActiveX use for web site access is entirely a matter of preference, I would personally recommend that all users of Microsoft e-mail applications alter their e-mail client security settings so that neither ActiveX or scripting language is supported in incoming messages. This can be done by setting the e-mail security zone to 'restricted'.

-Steve

Unwanted wildcard match

BROWN Nick <Nick.BROWN@coe.int>

Mon, 14 Jun 1999 09:46:41 +0200

I don't normally like to present individual bugs as RISKS, but this one just bit me and is so counter-intuitive that I felt I had to report it.

It appears that when Windows NT (and, I imagine, other long-filename-enabled Windows variants) matches a user-specified wildcard in a DOS prompt, it matches the wildcard against both the full filename, and the pseudo-8.3 format filename.

For example, in a directory I have two files:

Shortcut to V1.LNK

Shortcut to V2.LNK

However, these were created in reverse order, which means that their 8.3-emulated names were also created in reverse order. So DIR/X shows:

```
Shortcut to V1.LNK    SHORTC~2.LNK
Shortcut to V2.LNK    SHORTC~1.LNK
```

Now, I wanted to get rid of "Shortcut to V1.LNK", and a number of related files, so I typed

```
DEL *1.LNK
```

and "Shortcut to V2.LNK" disappeared as well.

The RISK ? With Microsoft, a wildcard can match a filename character that

you didn't even know was in the filename - indeed, which is part of a compatibility system which I don't need to use. (There is no way to predict

a file's 8.3-emulated name from its full name - another magnificent piece of non-design.)

Nick Brown, Strasbourg, France.

e-mail address updates : @coe.int replaces @coe.fr
for more information, <http://dct.coe.int/info/emfci001.htm>

Bank sued over client data sale

Monty Solomon <monty@roscom.com>
Tue, 15 Jun 1999 12:46:58 -0400

The state of Minnesota last week sued U.S. Bank for allegedly selling Social Security numbers, account balances and other sensitive customer data to a telemarketing company in exchange for commissions. Apparently several other banks are also hawking customer information, which raises serious privacy concerns. [Source: *ComputerWorld*, article by Kim S. Nash, 14 Jun 1999, <http://www.computerworld.com/home/print.nsf/CWFlash/990614AE82> PGN]

UAL -- the UnFriendly Cybersky?

David Leshner <wb8foz@nrk.com>
Mon, 14 Jun 1999 20:13:31 -0400 (EDT)

Recently, I went to check the status of an incoming UAL flight. The results were not encouraging. Their www page informed me:

Here is the latest information about the flight you selected. Note, the times listed are local airport times.

[United]Flight #1020
Departure Date: Dec 31, 1969

Status: Arrived

DEPARTS: San Jose, Costa Rica (SJO) ARRIVES: Mexico City, Mexico (MEX)
Left the Gate 6:10 am (Prev. day) (2 min Early)
Flight Arrived at Gate 9:45 am (Prev. day) (3 min Early)
Gate: N/A Gate: E

Status: Arrived

DEPARTS: Mexico City, Mexico (MEX) ARRIVES: Washington, DC (IAD)
Left the Gate 10:54 am (Prev. day) (2 min Early)
Estimated Arrival 3:51 pm (Prev. day)
Gate: 26 Gate: C9
Flight is on time.

=====

Besides the obvious Dec 31 1969, the page kept mentioning "Prev. Day" even though the flight was in the air at the time!

So I called the automated telephone status number. IT told the first leg of the flight was from not San Jose [SJO] but rather San Francisco [SFO].

So I ended up talking to a human. She took a surprisingly long time to check but said yes, it had originated from SJO and yes it was on time out of MEX. (It then arrived early...)

The RISK? The real rationale for the www page is the very low cost to service the query. But the ambiguity it created and the telco robot reinforced, drove me to the highest transaction cost method.

[See John Rushby's item in [RISKS-20.15](#). 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 20: Issue 45

Thursday 17 June 1999

Contents

- [eBay embarrassed by crash of system and plunge of stock](#)
[NewsScan](#)
- [Risks of e-mail borne viruses, worms, and Trojan horses](#)
[Bruce Schneier](#)
- [Not trusting virus scans](#)
[Paul Hoffman](#)
- [Risks of virus detectors blocking RISKS!](#)
[MAILsweeper](#)
- [Supremes uphold law barring indecent speech online](#)
[NewsScan](#)
- [Trouble for DoubleClick](#)
[Monty Solomon](#)
- [Human error called culprit in 3 rocket launch failures](#)
[Lindsay Marshall](#)
- [More troubles with PDF](#)
[Joe McCauley](#)
- [Re: A THAAD Day in Black Rock](#)
[Danny Cohen](#)
- [Re: GPS and collision risks](#)
[Peter B. Ladkin](#)

- [GPS and collision risks in marine navigation](#)
[Chris Bruce or Bruce Chris?](#)
 - [Re: Risks - Depending on a *.xxx convention for file types](#)
[Rumy Driver](#)
 - [More on "Unwanted wildcard match"](#)
[Nick Brown](#)
 - [REVIEW: "Corporate Espionage", Ira Winkler](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ eBay embarrassed by crash of system and plunge of stock

"NewsScan" <newsscan@newsscan.com>
Tue, 15 Jun 1999 07:25:48 -0700

The fallout from the 22-hour system outage last week of eBay, the popular Internet auction site, has resulted in an 18% tumble of that company's stock. Analysts seem to regard the technical problems as normal growing pains. Michael Bernstein of the Gartner Group regards eBay's technical and investor problems as relatively minor, and explains: "It's a fiasco like this that will force a company to really fix the problem." (AP/*San Jose Mercury News*, 14 Jun 1999; NewsScan Daily, 15 June 1999)
<http://www.sjmercury.com/svtech/news/breaking/merc/docs/000266.htm>

[Earlier eBay troubles were reported in [RISKS-20.38](#). PGN]

⚡ Risks of e-mail borne viruses, worms, and Trojan horses"

Bruce Schneier <schneier@counterpane.com>

Tue, 15 Jun 1999 16:48:25 -0500

Looking back from the future, 1999 will have been a pivotal year for malicious software: viruses, worms, and Trojan horses (collectively known as "malware"). It's not more malware; we've already seen thousands. It's not Internet malware; we've seen those before, too. But this is the first year we've seen malware that uses e-mail to propagate over the Internet and tunnel through firewalls. And it's a really big deal.

Viruses and worms survive by reproducing on new computers. Before the Internet, computers communicated through floppy disks. Hence, most viruses propagated on floppy disks, and sometimes on computer bulletin board systems (BBSs).

There are some obvious effects of floppies as a vector. First, malware propagates slowly. One computer shares a disk with another which shares a disk with five more, and over the course of weeks or months a virus turns into an epidemic. Or maybe someone puts a virus-infected program on a bulletin board, and thousands get infected in a week or two.

Second, it's easy to block disk-borne malware. Most anti-virus programs can automatically scan all floppy disks. Malware is blocked at the gate. BBSs can still be a problem, but many computer users are trained never to download software from a BBS. Even so, anti-virus software can automatically scan new files for malware.

And third, anti-viral software can easily deal with the

problem. It's easy to write software to block malware you know about. You simply have the anti-virus scanner search for bit strings that signify the virus (called a "signature") and then execute the automatic program to delete the virus and restore normalcy. This deletion routine is unique per virus, but it is not hard to develop. Anti-viral software has tens of thousands of signatures, each tuned to a particular virus. Companies release them within a day of learning of a new virus. And as long as viruses propagate slowly, this is good enough. My software automatically updates itself once a month. Until 1999, that was enough.

What's new in 1999 is e-mail propagation of malware. These programs -- the Melissa virus and its variants, Worm.ExploreZip worm and its inevitable variants, etc. -- arrive via e-mail and use e-mail features in modern software to replicate themselves across the network. They mail themselves to people known to the infected host, enticing the recipients to open or run them. They don't propagate over weeks and months; they propagate in seconds. Anti-viral software cannot possibly keep up.

And e-mail is everywhere. It runs over Internet connections that block everything else. It tunnels through all firewalls. Everyone uses it.

It's easy to point fingers at Microsoft. Melissa uses features in Microsoft Word (and variants used Excel) to automatically e-mail itself to others, and Melissa and Worm.ExploreZip make use of the automatic mail

features of Microsoft Outlook. Microsoft is certainly to blame for creating the powerful macro capabilities of Word and Excel, blurring the distinction between executable files (which can be dangerous) and data files (which, before now, were safe). They will be to blame when Outlook 2000, which supports HTML, makes it possible for users to be attacked by HTML-based malware simply by opening an e-mail. Microsoft set the security state-of-the-art back 25 years with DOS, and they have continued that legacy to this day. They certainly have a lot to answer for, but the meta-problem is more subtle.

One problem is the permissive nature of the Internet and the computers attached to it. As long as a program has the ability to do anything on the computer it is running on, malware will be incredibly dangerous. Just as firewalls protect different computers on the same network, we're going to need something similar to protect different processes running on the same computer.

This cannot be stopped at the firewall. This type of malware tunnels through a firewall using e-mail, and then pops up on the inside and does damage. So far the examples have been mild, but they represent a proof of concept. And the effectiveness of firewalls will diminish as we open up more services (e-mail, web, etc.), as we add increasingly complex applications on the internal net, and as crackers catch on. This "tunnel-inside-and-play" technique will only get worse.

And anti-virus software can't help much. If a virus can infect

1.2 million computers (one estimate of Melissa infections) in the hours before a fix is released, that's a lot of damage. What if the code took pains to hide itself, so that a virus won't be discovered for a couple of days. What if a worm just targeted an individual; it would delete itself off any computer whose userID didn't match a certain reference? How long would it take before that one is discovered? What if it e-mailed a copy of the user's login script (most contain passwords) to an anonymous e-mail box before self-erasing? What if it automatically encrypted outgoing copies of itself with PGP or S/MIME? Or signed itself; signing keys are often left lying around the system. Even a few minutes of thinking about this yields some pretty scary possibilities.

It's impossible to push the problem off onto users with "do you trust this message/macro/application" messages. Sure, it's unwise to run executables from strangers, but both Melissa and Worm.ExploreZip arrive pretending to be friends and associates of the recipient. Worm.ExploreZip even replied to real subject lines. Users can't make good security decisions under ideal conditions; they don't stand a chance against a virus capable of social engineering.

What we're seeing here is the convergence of several problems: the permissiveness of networks, interconnections between applications on modern operating systems, e-mail as a vector to tunnel through network defenses and

as a means to spread extremely rapidly, and the traditional naivete of users. Simple patches won't fix this. There are some interesting technologies on the horizon that try to mimic the body's own immune system to automatically deal with unknown malware, but I am not very optimistic about them. Sure they'll catch some things, but it will always be possible to design malware specifically to defeat the immune systems. A large distributed system that communicates at the speed of light is going to have to accept the reality of viral affections at the speed of light. Unless security is designed into the system from the bottom up, we're constantly going to be fighting a holding action.

Melissa:

<http://www.zdnet.com/zdnn/stories/news/0,4586,2233116,00.html>
<http://www.zdnet.com/zdnn/stories/news/0,4586,2234121,00.html>

Worm.ExploreZip

<http://www.zdnet.com/zdnn/stories/news/0,4586,2274306,00.html>
<http://www.wired.com/news/news/politics/story/20160.html>
<http://www.symantec.com/press/1999/n990614d.html>

Bruce Schneier, President, Counterpane Systems Phone: 612-823-1098
101 E Minnehaha Parkway, Minneapolis, MN 55419 Fax: 612-823-1590

Free crypto newsletter. See: <http://www.counterpane.com>

✉ Not trusting virus scans (Re: Karger, [RISKS-20.45](#))

Paul Hoffman / IMC <phoffman@imc.org>

Tue, 15 Jun 1999 14:21:42 -0700

[On the other hand,] I ran **two** virus checkers against an attachment I got last week, and both said it was fine, so I opened the attachment. It was the new ExploreZip worm. Virus checkers inherently don't work on viruses that are newer than your last update of the settings file. In this case, I had the latest version of both checkers, but the virus was "too new" for either of them.

Paul Hoffman, Director, Internet Mail Consortium

⚡ Risks of virus detectors blocking RISKS! (retitled by PGN)

<MAILsweeper@health.gov.au>

16 Jun 1999 07:51:24 +1100

[Original Subject: A copy of Melissa Virus may have been detected in a message]

[NOTE: At least the intended recipient was CC:ed. PGN]

CONTENT VIRUS ALERT!

This is an automated response to inform you that a potential Melissa computer virus (or variant) has been detected in an inbound electronic mail message to:

[...][@health.gov.au](mailto:owner-risks@csl.sri.com)

Date: Tue, 15 Jun 1999 12:07:31 -0700 (PDT)

From: owner-risks@csl.sri.com

[Subject: [RISKS-20.44](#)]

The message has been quarantined to prevent further propagation of the virus. Please remove the virus from the original document(s) or program(s) and send again. If you wish to discuss this matter, please contact the postmaster as indicated below.

Email: postmaster@health.gov.au

Phone: +61 2 6289 7828

Fax: +61 2 6289 4928

[So, which part of [RISKS-20.44](#) looked like Melissa herself? Presumably the CERT Advisory which told where to get the advisories? PGN]

[BankBoston Gatekeeper Server also blocked the issue, but did NOT

CC: the intended recipient. I also had a note from Lindsay Marshall

(who handles the RISKS redistribution for the UK); he also reported receiving such bounces. PGN]

Supremes uphold law barring indecent speech online

"NewsScan" <newsscan@newsscan.com>

Tue, 20 Apr 1999 10:20:26 -0700

The U.S. Supreme Court has upheld a lower court ruling that affirmed the constitutionality of a provision of the Communications Decency Act of 1996 that makes it a crime to transmit a "communication which is obscene, lewd, lascivious, filthy or indecent with intent to annoy, abuse, threat or harass another person." The provision had been challenged by a San Francisco

company that had developed the "annoy.com" Web site to let people send anonymous (and allegedly "indecent") messages to public officials. (AP 19 Apr 1999, <http://www.usatoday.com/life/cyber/tech/cte912.htm>; NewsScan DAILY, 20 Apr 1999)

✂ Trouble for DoubleClick

Monty Solomon <monty@roscom.com>
Tue, 15 Jun 1999 23:44:37 -0400

Barely 24 hours after DoubleClick said that it would acquire marketing research company Abacus Direct for \$1 billion in stock, privacy coalitions announced that they would file complaints with the FTC, contending that the merged entity would pose a threat to consumer privacy. The merger, which would help DoubleClick build the ultimate online database of consumers, brings the company closer than any other to achieving every online marketer's dream. But along the way, DoubleClick may have stumbled into a consumer-backlash nightmare.

[Jacob Ward: <http://www.thestandard.com/articles/display/0,1449,5017,00.html>]

✂ Human error called culprit in 3 rocket launch failures

<Lindsay.Marshall@newcastle.ac.uk>
Wed, 16 Jun 1999 12:38:34 +0100 (GMT)

<<http://www.flatoday.com/space/explore/stories/1999b/061699e.htm>> is a Florida Today article that claims that typos in software caused the loss of three rockets.

Lindsay <http://catless.ncl.ac.uk/Lindsay>

[The article claims that the 30 Apr 1999 Titan 4B failure ([RISKS-20.39](#)) is being blamed on a shifted decimal point in the software for the rocket's upper stage. PGN]

✶ More troubles with PDF

"Joe McCauley" <mccauley@davesworld.net>
Tue, 8 Jun 1999 09:56:01 -0500

The article in [RISKS-20.43](#) from Bryan O'Sullivan about troubles printing a PDF document reminded me of my own experience with PDF around tax time. I moved last year and had to file two different state tax returns in addition to my federal return. I downloaded some of the tax forms and publications I needed from the web, all of which were in PDF format, and ran into several cases of PDF forms that looked fine on my Win95 PC display but not so good when I printed them on a LAN-attached Laserjet printer:

- Some of the Federal publications and instructions printed without any spaces between the words (luckily the forms themselves came out fine, at least the ones I needed);
- The Illinois form IL-1040 was unusable; apparently it couldn't handle a

character graphic about halfway down the first page and didn't print any

of the rest of the form after that;

- Many of Massachusetts tax forms are color-shaded and use colored

areas in parts of the forms. When printed on a Laserjet, which doesn't

support color, all these colors were replaced by shades of gray, making

some parts of the forms difficult or impossible to read. Some of these problems may have been due to my local computing environment (though I think at least the Mass. forms should have been

available in non-color versions). All illustrate the risks associated with

assuming PDF is a stable and reliable format for online distribution of forms and documents.

Joe McCauley

✈ Re: A THAAD Day in Black Rock (PGN, [RISKS-20.43](#))

Danny Cohen <cohen@rand.org>

Tue, 15 Jun 99 13:34:38 PDT

Antimissile missile hits flying target on 7th try

An expensive experimental antimissile missile did Thursday what it had been

unable to do on six previous attempts: Hit a flying target. A white puff of

smoke in the southern New Mexico sky marked where the Army's Theater

High-Altitude Area Defense, or THAAD, missile struck a target missile, which

left a squiggly white trail of vapor just to the west. [Source: CNN item,

10 Jun 1999, <http://cn.com/US/9906/10/missile.test.ap/>

[RISKS always seeks good success stories -- although this one must qualify as only a relative success, considering the previous failures. However, we receive very few RISKS-relevant success reports, and do not want readers to conclude that there are no successes. But in the long run, it does seem that there are very few risk-free successes. PGN]

✉ Re: GPS and collision risks (Wood, [RISKS-20.44](#))

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Wed, 16 Jun 1999 14:03:09 +0200

> [...] 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.

Intuitively, I doubt this. Here's the reasoning.

To begin with, let us consider flight along, say, US Federal Airways.

Firstly, (a) separation in instrument meteorological conditions is ensured by ATC. No change in risk here. Secondly, (b) aircraft flying under instrument flight rules in visual meteorological conditions are flying in cruise at different altitudes (thousands of feet) than those flying under visual rules (thousands + 500 feet). Thirdly, although I cannot find it in

the US Aeronautical Information Manual (AIM), (c) pilots of aircraft flying visually on designated airways have *always* been advised to keep the airway centerline/fix to one side of them - yes, the same side (actually, this is well-known pilot lore all over). This takes care of the climb/descent problem. US Federal Airways extend horizontally to 4 nautical miles (4.6 statute miles) each side of the centerline.

Federal Airways are defined by VOR transmitters not more than 50nm from any point on the airway that they are defining. Even though a signal may be distorted, all receivers will be receiving the same distorted signal, so any individual variation must be in the individual receivers in the aircraft. I can see no way of demonstrating either that pilots fly more accurately to GPS guidance than they do to VOR guidance, or that VOR reception is generally sloppier than the accuracy to which visual pilots are flying an airway (my experience, in fact, is quite the opposite, as would be that of most instrument flight instructors trying to get their proteges to hold a VOR course, I would suppose!). Unless one or the other of these can be demonstrated, one could not conclude that flying behavior on airways had changed significantly with the introduction of GPS.

But suppose that one could demonstrate somehow that people were flying more accurately with GPS guidance. Then to conclude that the risk of collision was higher, one would have to show that the protocols (a)-(c) above were not in general being followed. Since (a) and (b) are enshrined in

aviation

regulations, and (c) in good practice/pilot lore, I doubt this would be easy to demonstrate.

One other way to show that the risk of midair collisions had increased would be to show that there had been more midair collisions since GPS use became prevalent, and that this was not just a statistical fluctuation. Well, I don't know for sure, but I don't think there have been more. Even if there had, the cause of the phenomenon would have to be determined, and for the above reasons it would be very hard to show that it was due to suddenly-increased accuracy of flying of VFR pilots.

So much for airways. On to other possibilities. Perhaps Wood was thinking of pilots wanting to fly to point X and lots of them all getting exactly to point X. If point X are the published GPS coordinates of an airport, there exist procedures to follow well before one gets to point X, which have been designed to alleviate the possibility of midairs in the neighborhood of an airport. One would have to imagine that somehow pilots are ignoring these procedures because they have a GPS, and I don't see how one could show any such thing. If point X is some specific sightseeing point, then I grant that there may be an increased need for vigilance since now one can navigate precisely to X. However, I don't know what the proportion of such flights would be, and I doubt that they are representative of most flights (It would seem appropriate to reiterate the usual warnings to pilots about increased traffic density in the vicinity of sightseeing attractions.)

Finally, I should note the article in Risk Analysis 17(2):237-248, 1997, by Robert Patlovany entitled U.S. Aviation Regulations Increase Probability of Midair Collisions, brought to my attention by Hal Lewis (who, by the way, has written a fine, fine book on making decisions called Why Flip a Coin?, New York: John Wiley & Sons, 1997, which I found very entertaining as well as enlightening and have promised for two years to review for Risks, but haven't yet. Hal's got a great writing style. Read it. So there). Patlovany uses "a purely stochastic Monte Carlo model [...] to compare the relative midair collision course probabilities and mean closing velocities of four systems of rules for aircraft cruising altitudes as a function of altitude error: (1) current U.S. federal rules, (2) random altitudes, and (3) [etc...] The calculations verify that (1) federal rules increase collision course probabilities by about four times more than for a chaotic system of aircraft cruising at randomly selected altitudes, (2) risk is directly proportional to the level of compliance, and (3) [etc]."

Note that Patlovany is considering cruising flight only, and altitudes, that is, vertical displacement, not the horizontal displacement which I take to be the relevant factor for evaluating Wood's GPS vs. VOR contention.

Prof. Peter Ladkin Ph.D., Univ. Bielefeld, Technische Fakultät, D-33501 Bielefeld (Germany) <http://www.rvs.uni-bielefeld.de> +49 (0)521 106-5326/5325

✂ GPS and collision risks in marine navigation (Re: Wood, [RISKS-20.44](#))

Bruce Chris <chris.bruce@hyder.com>

Wed, 16 Jun 1999 11:00:06 -0000

Lloyd Wood's comment regarding the probability of a collision between aircraft using GPS on established air routes applies equally to marine navigation. Navigation using electronic aids is generally from waypoint to waypoint. A "marine" waypoint is often a fairway buoy marking the end of a channel into a harbour or perhaps a buoy marking a shoal area at sea or a headland to be rounded. Vessels head from all directions towards the waypoints. A good lookout is necessary! This topic has had mention in the marine press for some years.

It also reminds me of the use of radar for collision avoidance at sea leading to what is known as Radar Assisted Collisions!

✂ Re: Risks - Depending on a *.xxx convention for file types

"Rumy Driver" <Rumy.Driver@sybase.com>

Wed, 16 Jun 1999 13:40:41 -0500

This is to note we are still paying for the archaic way of using the *.xxx extension for defining the file type.

This is only on Windows platforms which are a legacy of DOS days.

In most other platforms files have 2 parts (e.g. MacOS)

part1 resource fork

 Contains the actual meta-data - program that created file,
date of
creation, date of last modification

part2 data fork

 Actual data

Now in the DOS-legacy world it is soooo easy to rename a file to
another

extension and the file morphs itself. This is the sneaky trick/
way used to
spread the latest virus/worm.

Another suggestion for *.ZIP files is NOT to double-click them
and launch,

but to use the Classic mode of WinZip and check what is in the
ZIP archive

before extraction. This would have let people know that it's a
EXE file and

they could have taken precautions(?).

Another suggestion is not to have a completely homogeneous
environment

(reminiscent of the potato"e" (apologies to Dan Quayle) famine)

Rumy Driver, Sybase Technical Support

🔥 More on "Unwanted wildcard match" ([RISKS-20.44](#))

BROWN Nick <Nick.BROWN@coe.int>

Wed, 16 Jun 1999 18:45:08 +0200

I received quite a lot of mail on this subject. A couple of
people

helpfully tried to explain what they thought was the problem,
based on their

knowledge of DOS, but "assuming" that NT works that way, which

it doesn't.
(RISKS of assuming next-generation systems are infelicity-compatible, I guess.)

Yes, in DOS, the wildcards *1.LNK and *.LNK are identical, since DOS treats * to mean "everything up to the period" (and there can only be one period).
However, NT's wildcard matching does more or less what you'd expect - it's quite close to, say, how DCL does it under VMS. My problem is that it matches both the visible and the invisible filenames.

For example, if I do this:

```
C:\>copy afile.txt longname2.txt
C:\>copy afile.txt longname1.txt
C:\>copy afile.txt longname4.txt
C:\>copy afile.txt longname3.txt
C:\>dir /x long*.*
    LONGNA~2.TXT  LongName1.txt
    LONGNA~1.TXT  LongName2.txt
    LONGNA~4.TXT  LongName3.txt
    LONGNA~3.TXT  LongName4.txt
```

> and delete *1.TXT, I "only" lose the first two files.
>

Footnote: Microsoft have, however, faithfully re-implemented in NT the wonderful DOS bug whereby, if you change a file's extension while copying it using a partial-match wildcard, the copy is done as if you said /A for ASCII. For example, if I have WINWORD.EXE and I want to copy it to NICK.XXX and I'm feeling lazy, I might say
> COPY W*.EXE NICK.XXX
without putting the /B switch on the COPY command.

> Try it - you'll get a file truncated to the offset of the first ctrl-Z

> character in the original.

Thanks also to the person who pointed out that the automatic note appended to all outgoing e-mails from our site (saying that our domain name has changed), which PGN didn't chop off as he sometimes does with voluble sigs, contained a reference to a site which didn't work. Apparently this went wrong about two weeks ago. Of the 80000 or so Internet E-mails we have sent out since then, nobody else has bothered to mention the problem. This must mean something.

Nick Brown, Strasbourg, France <http://dct.coe.int/info/emfci001.htm>

⚡ REVIEW: "Corporate Espionage", Ira Winkler

Rob Slade <rslade@sprint.ca>
Tue, 15 Jun 1999 08:39:25 -0800

BKCRPESP.RVW 990424

"Corporate Espionage", Ira Winkler, 1997, 0-7615-0840-6,
U\$26.00/C\$34.95
%A Ira Winkler
%C 3875 Atherton Road, Rocklin, CA 95765-3716
%D 1997
%G 0-7615-0840-6
%I Prima Publishing
%O U\$26.00/C\$34.95 800-632-8676 916-632-4400 fax: 916-632-1232
%P 365 p.
%T "Corporate Espionage"

This readable and realistic guide to becoming professionally paranoid has a

special emphasis on data security and high tech companies, but can be very useful to pretty much anyone.

Part one looks at espionage concepts. Chapter one, and the introduction that precedes it, points out that information is one of the primary sources of value in any business. Chapters two through five look at the basic ideas for any examination of data security, those of risk, value, threat, and vulnerability. Presented in terms, and with examples, that anyone can understand, they nevertheless form the foundation for examining security and protection for computer and communications systems as well as the sales "red book" for next quarter.

Part two presents a variety of case studies. Winkler concentrates on the non-technical, relatively simple, and devastatingly effective "social engineering" aspect of break-ins. Chapter six is a compilation of tactics used in various penetration tests. One particular test is outlined in chapter seven. Chapters eight to eleven detail actual espionage cases carried out by foreign companies. A different penetration test is presented in chapter twelve. A third party account of a "crack" is discussed in chapter thirteen.

Part three outlines what you can do to protect yourself. Chapter fourteen describes a significant list of countermeasures to take, starting with an effective education program. Finally, chapter fifteen presents a large scale program for overall security.

This book is very down to earth, and very real. Unlike any number of "hacker" books, it doesn't attempt to impress the reader with displays of arcane knowledge: it doesn't have to. Technical details are almost non-existent, making the text an excellent choice for use in educating any level or type of employee on the need for security.

copyright Robert M. Slade, 1999 BKCRPESP.RVW 990424
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

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



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 46

Saturday 19 June 1999

Contents

- [NASA discloses space station blunder](#)
[SigmaXi ScienceInTheNews](#)
- [Y2K test sends sewage flowing in Los Angeles](#)
[Henry Baker](#)
- [Resetting the A320 computer](#)
[Diomidis Spinellis](#)
- [Intuit/Quicken Force Users to Internet & MS Internet Explorer](#)
[Lauren Weinstein](#)
- [MS Word not as helpful as it thinks](#)
[Bill Shymanski](#)
- [YANTBOF: yet another NT buffer overrun flaw](#)
[Epstein Jeremy](#)
- [New ATM hazard](#)
[Aahz Maruch](#)
- [Yet another ATM scam](#)
[Mike Williams](#)
- [The cell phone that wouldn't stay OFF](#)
[Michael Heilman](#)
- [Another case of credit-card 'security'](#)
[David Alexander](#)

- [Maldesigned computer system slows background checks](#)
[Kragen Sitaker](#)
 - [Factoid paranoia](#)
[Mike Giroux](#)
 - [Risks of keywords in CSV files](#)
[Rex Black](#)
 - [REVIEW: "Intrusion Detection", Edward G. Amoroso](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **NASA discloses space station blunder**

inthenews <inthenews@SIGMAXI.ORG>

Fri, 18 Jun 1999 11:39:49 -0400

A blunder by flight controllers prevented the new international space station from moving out of the way of dangerous space junk. The rocket debris ended up passing at a safe distance. NASA said the sequence of computer commands sent up by flight controllers to fire the station's engines over the weekend failed because of human error. It disclosed the incident Thursday.

Initially, the U.S. military organization that tracks objects in space predicted the rocket chunk would pass within two-thirds of a mile of the space station on Sunday. It ended up coming no closer than 4 1/2 miles.

<http://www.latimes.com/HOME/NEWS/WIRES/WHEALTH/tCB00V0366.html>

[*The Los Angeles Times, 18 Jun 1999*; From SCIENCE-IN-THE-NEWS]

Sigma Xi Homepage <http://www.sigmaxi.org>

Media Resource Service <http://www.mediaresource.org>

American Scientist magazine <http://www.sigmaxi.org/amsci/amsci.html>

⚡ Y2K test sends sewage flowing in Los Angeles

Henry Baker <hbaker@netcom.com>

Fri, 18 Jun 1999 06:45:45 -0700

A supposedly routine test of LA's Y2K readiness of the emergency preparedness system at the San Fernando Valley sanitation plant caused about 4 million gallons of raw sewage to be dumped into the Sepulveda Dam area. A gate to a major sewer pipe closed without warning because of a programming error. [Source: article by Miguel Bustillo, Karima A. Haynes, Patrick McGreevy, <http://www.latimes.com/HOME/NEWS/Front/t000054865.html>, *L.A. Times*, 18 Jun 1999; PGN-ed]

⚡ Resetting the A320 computer

Diomidis Spinellis <dspin@aegean.gr>

Sat, 19 Jun 1999 03:05:01 +0300

I was travelling from Athens to Munich on Lufthansa flight LH 3425 on 16 Jun 1999. Shortly before taxiing for takeoff, our A320 plane left the runway and moved aside. The captain immediately informed us that we were having a slight technical problem that they would try to rectify and that we would be given further information in a short while. About five minutes later the following announcement was made:

"Ladies and Gentlemen this is your captain again. We had to reset two of our computers and now it is looking real fine again."

During the flight the crew kindly allowed me to talk to the first officer about the incident. My prepared list of questions concerned the problem domain, its criticality, frequency of occurrence, and reporting procedures.

According to the captain, the problem occurred on a flight control computer (ELAC1) and involved erroneous position monitoring of the right elevator.

The officer assured me that the problem was not critical, occurred on only one of four different reports and although it was part of a ground checklist it would not have been a problem during the flight. I was told that such problems sometimes do occur and that the problem had already been reported by telex to the airline's maintenance base.

Here is a verbatim - I hope - transcription from a printed log I was shown:

```
F/CTL servo fault
R Elevator POS MON XDLR
```

(Disclaimer: I am not an aviation expert; the report is my - perhaps limited - understanding of the captain's answers.)

The risks? As far as I know modern flight-control computers do not need a reset before takeoff*, nor should a reset be needed after a human operator error. Obviously a software or hardware fault had caused the computers to malfunction. Since resetting a computer does not typically isolate and

correct faults (otherwise Windows would long have reached a 0% defect rate),
we were flying on a plane with a known and demonstrated software fault.
Although the problem manifestation was on a non-critical area, we all know that the underlying cause could well result in more serious side-effects since it occurred on a critical flight control component. More worryingly, this appeared not to be a singular event.

[*] Interestingly the Space Shuttle software does need to be reloaded between different flight phases. A fascinating description can be found in Gene D. Carlow. Architecture of the space shuttle primary avionics software system. Communications of the ACM, 27(9):926-936, September 1984.
Diomidis Spinellis, University of the Aegean

✶ Intuit/Quicken Force Users to Internet & MS Internet Explorer

Lauren Weinstein in PRIVACY Forum <privacy@vortex.com>
Sat, 19 Jun 99 12:22 PDT

PRIVACY Forum Digest Saturday, 19 Jun 1999 Volume 08 :
Issue 09

Moderated by Lauren Weinstein (lauren@vortex.com)
Vortex Technology, Woodland Hills, CA, U.S.A. <http://www.vortex.com>

Date: Sat, 19 Jun 99 09:46 PDT
From: lauren@vortex.com (Lauren Weinstein; PRIVACY Forum Moderator)
Subject: Intuit/Quicken Force Users to Internet & MS Internet Explorer

Greetings. Just as the banking industry in the U.S. has been issuing concerns about the security of Internet and Web-based banking systems, one of the biggest players in the online banking industry, Intuit, makers of Quicken, have quietly moved to force all of their users onto the Internet for all online banking services, and in some cases are requiring the use of Microsoft's Internet Explorer instead of other browsers such as Netscape Navigator.

Catherine Allen, chief executive of the Banking Industry Technology Secretariat, a division of Bankers Roundtable, recently said, "The banks feel that firewalls and what they have internally is in great shape, but the link is to the consumer and PC environments [where they find security more suspect]."

While newer versions of Quicken software have apparently been Internet-based for some time, many users had opted to stay with older versions since they used direct dialup lines for communications, and did not rely on Microsoft's Internet Explorer.

However, Intuit (and/or in some cases users' banks) over the last two months or so have been sending out a somewhat confusing series of letters, informing these users that their versions of Quicken are not "Y2K" compliant, and that they must upgrade by designated nearby dates (e.g. June 30, 1999) or lose their online banking access. Some materials simply suggested that certain

features (such as pre-scheduled bill payments) would have problems past

Jan 1 2000--other materials claimed a total cutoff of services to non-upgraded users. Sometimes the same letter seemed to make both statements.

Intuit and/or user banks made a number of options available, including a free minimalist downloadable upgrade and various payment-based enhanced upgrades. However, the fine print of these offers (sometimes buried at the end of the letters) indicated that all access would be via the Internet for these new versions. Arrangements for limited free Internet access would be available to those who didn't already have an Internet Service Provider, the letters suggested.

I spent a couple of weeks clarifying this whole situation with Intuit and their public relations firm through a lengthy series of phone calls. While it wasn't difficult reaching Intuit's public relations folks, getting to people who could answer technical questions at this level was a bit more of an effort. However, everyone involved was polite and willing to address my questions in a direct manner to the extent that they could.

The bottom line is that all users of older Quicken software *do* need to upgrade and *will* be using the Internet for all future transactions. There will be limited free Internet access available for Quicken transactional use (I believe an hour a month, which would be sufficient for this purpose) for people who need the service. It is a bit unclear how long this free access would be available--one person suggested indefinitely, but this

does not
appear to be a guarantee.

I'm told that existing users doing the minimalist upgrade from older Quicken versions (e.g. Version 5 for Windows) will not need to install or use Internet Explorer (IE) for most online operations. Users of the more sophisticated upgrades may be required to use IE for more functions, and *all* new users of Quicken will be required to install and use IE for secure signup--Intuit claims that Netscape doesn't have the "required" functionality for this purpose.

I'm also told that the "standard" installation option of many or all of these new Quicken versions will install IE by default. This means that if you do not want an IE installation (and if you're in a category of existing user that doesn't need it) you would probably have to disable the IE installation via the "custom" installation options of the Quicken setup program. This could be particularly important to users who may be concerned about losing existing associations and defaults for any other web browser already installed (which may be affected by an IE installation), or where security concerns over IE's ActiveX functions and other related system complexities are present.

I have in the past expressed other concerns with Quicken. A continuing problem is that if online banking transactions are not downloaded at frequent enough (unannounced) intervals, transactions will be silently lost and all related calculations and records from that point onward will be

in error
unless manually corrected. Intuit's response to this issue continues to be suggesting that users have paper records to fix such problems, and that most users access their data frequently enough that it isn't an issue for them. Frankly, I would argue that this rather negates much of the point of using the software in the first place, if you can't trust the transaction record, even if relatively few people might be affected by this particular undocumented problem! I did by the way again suggest (this time to a Quicken product manager) that users at *least* be warned when transactions have been lost--they again said they'd consider it...

So, if you're a Quicken user, and you've recently been told you need to upgrade due to that mean old Y2K monster, you're not alone if the situation seemed a bit confusing based on the materials you received in the mail.

PRIVACY Forum Digest V08 #09, Lauren Weinstein --- <http://www.vortex.com>

Host, "Vortex Daily Reality Report & Unreality Trivia Quiz" --- <http://www.vortex.com/reality>

⚡ MS Word not as helpful as it thinks

Bill Shymanski <wtshyman@mb.sympatico.ca>
Sat, 19 Jun 1999 13:33:09 -0400

I recently helped edit a specification, in which a list of items to be supplied had the wrong quantities shown. It turns out Microsoft

Word 97

though that the list beginning "1 Rack", and continuing on from there, was supposed to be a numbered list - so Word "helpfully" automatically incremented what was meant to be the quantity field as if it were sequence numbers of a list. Luckily this was caught at draft stages, but the risk of getting quantities wrong is present.

On the whole, I find that features of this nature cost more time than they save; the software is never smart enough to figure out what I really want and when it guesses, it usually gets it wrong. I'd sooner type my own numbered lists than fight with the word-processor. Automatic renumbering is also fairly useless if you happen to refer elsewhere in the document to, say, item 3.4.5 and Word has renumbered it after the reference was created.

W. T. Shymanski <wtshyman@mb.sympatico.ca>

⚡ YANTBOF: yet another NT buffer overrun flaw

"Epstein, Jeremy" <Jeremy_Epstein@NAI.com>

Fri, 18 Jun 1999 06:53:49 -0700

Just in case anyone hasn't seen it already:

<http://www.eeye.com/database/advisories/ad06081999/ad06081999.html>

for the technical info, or

<http://www.wired.com/news/news/technology/story/20285.html>

for a higher-level description.

This was also mentioned briefly in **The Washington Post**, 18

June 1999.

--Jeremy

[And Microsoft is accusing eEye of unfairly releasing information on this flaw, whereas eEye is claiming they notified MS -- which did not fix it rapidly enough. The obvious comment must be Old McRosoft had affirm: eEye, eEye, Owe!
See http://www.excite.com/computers_and_internet/tech_news/zdnet/?article=/news/19990617/2277295.inp
PGN]

⚡ New ATM hazard

Aahz Maruch <aahz@netcom.com>
Thu, 17 Jun 1999 09:30:08 -0700 (PDT)

UTM Systems (<http://www.utmsystems.com/>) is offering a new ATM card reader that goes into the floppy drive of a PC. I wonder how easy it'll be to crack the system to collect passwords -- they're advertising it for use in point-of-sale systems.

⚡ Yet another ATM scam

"Mike Williams" <mikew@harlequin.co.uk>
Wed, 16 Jun 1999 11:13:05 +0100

There was report in the Preston Citizen (Lancs. UK) last week about a new

ATM scam. This has taken place at ATMs at large supermarkets. Basically, 'devices' have been added to the exterior to get the pin number and read the card's magnetic strip -

'One device is an invisible key pad which is placed over the existing keys, which records the pin number, while another invention placed over the card slot copies the data on a magnetic strip. ... Because the user gets the card back and the cash requested they believe nothing is wrong. ... Police fear hundreds of local people have been affected by the scam. ... "We have talked to around 200 victims locally, most of who have been losing varying amounts in 250UKP sums."'

The bank has reportedly put a warning on its ATMs (I don't use there ATMs) warning customers to be on the lookout, and advises customers that if '... they see anything suspicious on a machine they should not use it.'

It seems supermarket ATMs were targeted since the crooks can easily keep an eye on them from the car park, plus have unobserved access to them at night - the supermarkets are usually on the edges of towns with minimal lighting.

No need to point out the risks ...

⚡ The cell phone that wouldn't stay OFF

<Michael_Heilman@infoimage.com>

Thu, 17 Jun 1999 13:06:08 -0400

My wife and I received a very long, very unusual message on our answering machine one day. Under a complex layer of foreground noises, there was a discernible conversation being recorded. After listening to it several times and recognizing personally significant phrases, we were quite concerned. It took several puzzling hours to realize what had happened: my wife had slipped her cell phone into her purse and as we were walking down the street, something pressed against the re-dial and called our home phone. Our answering machine recorded our muffled conversation under a layer of noises from the phone rubbing and jostling.

The RISK became apparent a couple of week later when my wife received a call from a business colleague asking if she had just called him back after their conversation, because he had just overheard the strangest sounding phone call. Well, what he heard, by the same mechanism, was my wife discussing, with someone else, her previous conversation with him right after hanging up and putting her phone away. Luckily, she had had nothing derogatory or confidential to say!

Looking for a solution: the phone has a keyboard lock that requires pressing 1-2-3 to unlock ... pretty good, but not foolproof. If the phone is turned off, it is very easy for it to get turned back on--just a quick press of one button.

⚡ Another case of credit-card 'security'

David Alexander <dave_ale@online.rednet.co.uk>

Wed, 16 Jun 1999 10:19:53 +0100

Yesterday I telephoned my credit card company to make some enquiries about various options they were offering. It was the first time I had called them for at least a year. Imagine my surprise when I was first asked to enter my credit card number in full and then informed that 'in order to improve security I needed to decide on a 4 digit number to be used to verify who I was in future'. I was then asked for my date of birth and the expiry date on my card as proof of who I was before being allowed to give them a number.

Hopefully the alarm bells have already gone off in your heads like they went off in mine. The whole idea is so full of holes and risk. Anyone who has accepted my card will have the full number and expiry date. Here in the UK you can get a copy of a Birth certificate with minimal difficulty, so anyone could ring up purporting to be me and 'swipe my identity' [pun intended]. I haven't sat and thought through in detail exactly what scams they could then pull off by telephone in terms of obtaining items by deception or simply wrecking my relationship with the company.

Be careful what you do on the phone.

David Alexander, Camberley, England, Founder member, European Top Methanol

Racers Association http://home.rednet.co.uk/homepages/dave_ale/dave_ale.html

✦ Maldesigned computer system slows background checks

Kragen Sitaker <kragen@pobox.com>

Tue, 15 Jun 1999 17:23:26 -0400 (EDT)

I expected to see this in the latest RISKS. It appeared in USA Today on 1999-06-03, page 1A and 2A, in an article entitled, "Pentagon crisis: Security-check backlog." Amid discussion of various kinds of mismanagement, agency politics, and the effects of the backlog (capsule summary: people like me who have security clearances get them by filling out some forms and then having Defense Security Service people chat with everyone they've known for the last ten years, and the process takes way too long), there was this juicy tidbit:

That flap was nothing compared to the problems that have emerged in the past eight months, since the security service turned on its new computer system at its Baltimore operations center. The Case Control Management System, or CCMS, [outgoing DSS director Steven] Schanzer says, was designed to "automate the management of the investigative process." But, say DSS officials, the system isn't working and there is no backup operation in place. [It's not clear whether they decommissioned an older computer system without thorough testing of a new one, or whether they just didn't have an older computer system that did the things this one does.]

Last April, the computer system crashed for four days, meaning ... "no

internal or external customers could get information from the system."

Schanzer says the problem is simple: the system choked on paper. It was

designed to take electronic questionnaires from security applicants, but

it was deluged with tens of thousands of paper submissions.

Another problem: The agency assumed applicants would fill out the forms

correctly. In many cases, that hasn't happened, and the system can't

detect the errors, Schanzer says. [Is this connected to forms being

filled out by hand instead of via EPSQ, which won't allow submission of

forms with certain kinds of errors? Or is this a separate problem? Is

this related to the crash?]

There is yet a third problem. Schanzer says the agency now has figured

how to get the paper through the system, but once a case is completed, it

takes about 20 days to get a print-out. [What? Why? No clues here.]

... "It should take no time at all," he explains. [...]

"We are bringing on an independent team to assess where we are with the

computer system," he [John Hamre, deputy Secretary of Defense] says. "I

need to know if we are barking up an empty tree" with the existing system,

or whether it should be replaced.

Earlier parts of the article explain that many, many people are getting paid

to sit around and do nothing until their clearances are granted (or denied,

in which case they are fired), and that soon, some classified contracts will cease to progress until clearances are granted, and that the NSA has recently gotten an exemption from the Pentagon to hire PIs to do the NSA's background checks, instead of relying on DSS.

The RISKS are not clear here, due to (what appears to be) USA Today's usual shoddy reporting. It sounds like the usual problem of undue reliance on untested software that was designed without reference to real life.

<kragen@pobox.com> Kragen Sitaker <<http://www.pobox.com/~kragen/>>

Factoid paranoia

Mike Giroux <rmgiroux@hotmail.com>
Tue, 15 Jun 1999 05:25:14 PDT

An interesting research project is described at

<http://www.research.digital.com/wrl/projects/Factoid/index.html>

Basically, this is a device that would log all of the small "factoids" that a person passes by each day (broadcast by other factoid devices in billboards or business cards, for instance), and then upload them into a home database in a secure way at any opportunity.

This system is only in the theoretical stages, so this isn't an urgent problem. However, my worry about the factoid system is about the "subpeona-bility" of the home database. Would you want a step-

by-step

record of where you went and who you saw each day of your life available to anyone who wants to start a nuisance civil suit against you?

Apart from that concern, though, it looks like a cool toy, and maybe even a useful tool. Maybe if "factoid privilege" were part of the law, this thing could take off.

Mike

⚡ Risks of keywords in CSV files

Rex Black <rexblack@ix.netcom.com>

Tue, 15 Jun 1999 17:20:34 -0500

Here's a fun "file portability" bug that sucked up a couple hours of my day.

1. Create a comma-separated variable file with three or four variables.
2. Name the first column "ID".
3. Try to import the file into Excel 97. You will receive a "Sylk: File format invalid" error.
4. Rename the first column "BugID".
5. Repeat step three. No problem.

I'm guessing that the file import facilities use the word "ID", if it occurs in the first two bytes of a file to be imported, as a keyword meaning, "The next few bytes will tell you what type of file this is." When the next few

bytes are just the headers for the rest of the columns, Excel pukes.

The Risk? In my opinion, this is the old "laconic/cryptic error message"

risk. Had the error message said, "Keyword 'ID' followed by invalid type,"

I would have gotten it right away. Instead, I went off on a wild goose

chase involving fix-width columns, tab-separated columns, and the like,

before I tried twizzling the header and--behold!--it worked.

Rex Black Consulting Services, Inc., 7310 Beartrap Lane, San Antonio,

TX 78249 +1 210 696 6835 <http://www.RexBlackConsulting.com>

★ REVIEW: "Intrusion Detection", Edward G. Amoroso

Rob Slade <rslade@sprint.ca>

Thu, 17 Jun 1999 08:43:56 -0800

BKINTDET.RVW 990423

"Intrusion Detection", Edward G. Amoroso, 1999, 0-9666700-7-8, U \$49.95

%A Edward G. Amoroso eamoroso@mail.att.net

%C P. O. Box 78, Sparta, NJ 07871

%D 1999

%G 0-9666700-7-8

%I Intrusion.Net Books

%O U\$49.95 973-448-1866 fax: 973-448-1868 order@intrusion.net

%P 218 p.

%T "Intrusion Detection"

This is not (very much not) to be confused with the identically named, and

almost equally recent, book by Escamilla (cf. BKINTRDT.RVW).

Where

Escamilla's is basically a large brochure for various commercial systems, Amoroso has specifically chosen to avoid products, concentrating on concepts, and not a few technical details. The text is based on material for an advanced course in intrusion detection, but is intended for administrators and system designers with a security job to do.

Chapter one, after demonstrating that the term means different things to different people, gives us an excellent, practical, real world definition of intrusion detection. This is used as the basis for an examination of essential components and issues to be dealt with as the book proceeds. Five different processes for detecting intrusions are discussed in chapter two. Each method spawns a number of "case studies," which, for Amoroso, means looking at how specific tools can be used. (This style is far more useful than the normal business case studies that are long on who did what and very short on how.) Intrusion detection architecture is reviewed in chapter three, enlarging the conceptual model to produce an overall system. Chapter four defines intrusions in a way that may seem strange, until you realize that it is a very functional description for building detection rules. The problem of determining identity on a TCP/IP internet network is discussed in chapter five, but while the topic is relevant to intrusion detection, few answers are presented. Correlating events is examined in chapter six. Chapter seven looks at setting traps, primarily from an information gathering perspective. The book ends with a look at response in

chapter
eight.

The bibliography is, for once, annotated. While I do not always agree with Amoroso's assessments; I think he tends to give the benefit of the doubt to some who primarily deliver sensation; the materials are generally high quality resources from the field. Books and online texts are included, although the emphasis is on journal articles and conference papers.

The content is readable and, although it seems odd to use the word in relation to a security work, even fun. I suppose, though, that I must point out that your humble "worst copy editor in the entire world" reviewer found a significant number of typographic errors. (And some that can't be put down to typos: I think you'll find that it's "berferd" rather than "berford.")

This book works on a great many levels. It provides an overall framework for thinking about security. It thoroughly explains the concepts behind intrusion detection. And it gives you some very practical and useful advice for system protection for a variety of operating systems and using a number of tools. I can recommend this to anyone interested in security, with the only proviso being that you are going to get the most out of it if you are, indeed, responsible for designing network protection.

copyright Robert M. Slade, 1999 BKINTDET.RVW 990423
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

[http://victoria.tc.ca/techrev
~rslade](http://victoria.tc.ca/techrev/~rslade)

or

<http://sun.soci.niu.edu/>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 47

Saturday 10 July 1999

Contents

- [Electronics startup transient kills spacecraft](#)
[Craig DeForest](#)
- [NASA discloses space station blunder](#)
[Wayne Mesard](#)
- [Space Station AOL hack](#)
[Marc Passy](#)
- [Busy phone lines block stay of execution](#)
[Joe Thompson](#)
- [E-mail writer arrested for starting panic](#)
[Matthew Todd](#)
- [Garciparricide in All-Star balloting?](#)
[PGN](#)
- [Custodiet ipsos custodes? Not without permission!](#)
[Adam Shostack](#)
- [Singapore exchange blames outage on network failure](#)
[Paul Walker](#)
- [eBay outage traced to failure to upgrade](#)
[Steve Klein](#)
- [Australian virtual reality kanga-rues the day](#)
[Lindsay Marshall](#)

- [Faulty vending machines block emergency calls in Australia](#)
[Mark Nottingham](#)
 - [Brazilian telephone network chaos](#)
[Matthew Todd](#)
 - [Spell-checker run amok? Shandling-->Changeling](#)
[Jim Griffith](#)
 - [REVIEW: "Computer Security", Dieter Gollmann](#)
[Rob Slade](#)
 - [REVIEW: "Securing Java", Gary McGraw/Edward W. Felten](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Electronics startup transient kills spacecraft**

<craig@deforest.org>

Tue, 29 Jun 1999 10:27:17 -0700

A recent (25 Jun 1999) press release from NASA HQ identifies the untimely demise of the Wide Field Infrared Explorer (WIRE) spacecraft as due to a design flaw in the pyro control logic board. WIRE's detector was to be cooled with a block of solid hydrogen. The telescope cover's explosive release mechanism fired immediately when the instrument was powered up, exposing the detector to direct sunlight and sublimating all of the solid hydrogen on board within 48 hours of its 5-Mar-99 launch. Unbalanced thrust from the hydrogen venting gave the spacecraft an uncontrolled 60 RPM spin.

The telescope cover was ejected prematurely because "the transient performance of components was not adequately considered in the [electronics] design. ... The start-up time of the ... clock oscillator was not taken into consideration, leaving the circuit

in a non-deterministic state for a time sufficient for pyrotechnic actuation", according to the executive summary of the failure investigation report.

Contributing factors in the program included the lack of any peer review for the pyro box design (due to it not being completed at the time of the spacecraft SDR), insufficient interlocks in the pyro control circuits, and low fidelity of the ground support equipment used for preflight testing.

The executive summary of the report is available on the World Wide Web at "ftp://ftp.hq.nasa.gov/pub/pao/reports/1999/wire_summary.pdf".

Better, faster, cheaper: choose any two.

Craig DeForest

✈ NASA discloses space station blunder ([RISKS-20.46](#))

<Wayne.Mesard@East.Sun.COM>
Tue, 22 Jun 1999 17:22:01 -0400

> NASA said [the station's engines failed to fire]
> because of human error.

> Initially the rocket chunk [was predicted to] pass within two-thirds
> of a mile of the space station on Sunday. It ended up coming
> no closer
> than 4 1/2 miles.

Isn't this latter fact the real risk here? What is the average predictive error for space debris near-misses? Since we are counting on the accuracy

of these predictions to protect people and expensive equipment,
I would hope
it is less than 575%.

Space Station AOL hack

Marc P <passy#no_spam#@flex.net>

Tue, 29 Jun 1999 22:58:55 -0500

The server on which the International Space Station Problem Reporting database resides was recently "hacked," prompting its disconnection from *all* networks, including the local LAN, for security upgrades. This database is used by the hundreds of users here at Johnson Space Center and at the various development sites around the country to document problems and direct fix work with hardware, software, and documentation for all parts of the ISS

Similar to problems AOL has had, it seems that someone, most likely someone involved with the ISS program, obtained the name of a user with administrator access, then called the help desk and asked for a password reset. They were promptly given that new password, after which they proceeded to do something objectionable with the password file. (That part's still not quite been released.)

It doesn't appear that the database was damaged, but the access removal brought productive work reviewing problems and working fixes almost to a standstill.

Aside from other measures, and to add insult to injury, they are asking for a "PIN" to use to help identify the user if they call for resets. They asked that these "PINs" be chosen by the user and sent via CLEAR TEXT E-MAIL!!!!!!!

Besides which, if I forget a password that I use every couple of days, and I call for a reset, how am I going to remember a "PIN" that I specified six months before???

To reach me, you might try passy (at) flex (dot) Net.

✶ Busy phone lines block stay of execution

Joe Thompson <joe@orion-com.com>
Fri, 25 Jun 1999 11:18:52 -0700 (PDT)

<http://www.cnn.com/WORLD/asiapcf/9906/25/philippine.execution.02/>

Summary: Due to phone problems, a stay of execution by the Philippine president could not be delivered in time to save the condemned prisoner. By the time the president's office got through to the prison, the lethal injection had already been administered. From the published details it's unclear whether the phone lines were misdirected in the system, or the president's office was calling the wrong number. -- Joe

Joe Thompson, Charlottesville, VA joe@orion-com.com
<http://kensey.home.mindspring.com/>

[Also noted by Robert Franchi in *The Boston Globe*, 18 Jun 1999:

He was scheduled to be executed for raping his own daughter. The governor of the Philippines finally relented to grant a stay of execution 5 minutes before the scheduled time. He could not get through on the phone or fax, and when he finally did get through, the man had been dead of lethal injection for 1 minute.
PGN]

✉ E-mail writer arrested for starting panic

"Matthew Todd" <matthew@mail.cmb.ac.lk>
Thu, 8 Jul 1999 13:25:40 +0600

Jose Omar Olaya, 24, was arrested for sending false e-mail messages from Hotmail urging everyone to take their money out of Davivienda Bank because of a pending government intervention. In the resulting panic, \$11.4M was withdrawn in one day, and the Columbian government had to cover the outflux.
[Source: AP item in **The Island**, 6 Jul 1999, from Bogota; PGN-ed]

RISKS and QUESTIONS:

1. The obvious one of spreading unsubstantiated rumours by email, which applies equally to financial information or computer viruses, or anything else.
2. Since Hotmail accounts are notoriously anonymous, how was this tracked back to him so that he could be arrested?

[Anonymity is generally only a relative concept. Who pays the

bills? PGN]

⚡ **Garciaparricide in All-Star balloting?**

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

Fri, 9 Jul 1999 11:22:48 -040

Boston Red Sox shortstop Nomar Garciaparra was running behind in the open balloting. As part of a huge last-day Internet deluge, Sox fan Chris Nandor cast 25,259 votes for him and other Red Sox players via the Internet. (Just a little Perl script.) However, the administrators of the balloting were able to detect the violation of the 22-vote maximum, because he used the same e-mail address each time, the same bogus phone number and zip code. (that's NAND-OR logic?) However, Garciaparra managed to pull from behind in other late votes that were apparently legitimate. [Source: PGN-ed from numerous media reports on 7 Jul 1999 from several contributors, including PGN who saw it in **The Boston Globe** and **The New York Times**.] One might wonder how many multiple votes were NOT caught.

⚡ **Custodiet ipsos custodes? Not without permission!**

Adam Shostack <adam@bindview.com>

Sun, 4 Jul 1999 06:35:20 -0400

In the case of Michael Hyde vs Abington (Massachusetts), Mr. Hyde was found

guilty of violating state wiretap laws, which forbid recording the voice of a person without their knowledge. Mr Hyde recorded the police being abusive towards him, using profanity threatening him with jail. When he brought the tape to the Abington police, they charged him with violations of the wiretap statue. He has been sentenced to six months probation and a \$500 fine.

It seems clear that if it is not possibly to surreptitiously monitor the police for abuse of their powers, such abuses are less likely to be caught and corrected.

The Boston Globe is very bad about maintaining URLs, but try http://www.boston.com/dailyglobe2/184/metro/Driver_guilty_in_taping_of_police%2b.shtml

✦ Singapore exchange blames outage on network failure

"Walker, Paul (India)" <paul_walker@in.ml.com>
Mon, 21 Jun 1999 12:32:23 +0530

Well, I am glad to see that the powers-that-be had:

- a contingency plan in place
- someone to oversee the Friday evening test has complete successfully
- excellent error messages to allow the operators to quickly identify the cause of the problem
- someone involved with the process with an overall understanding on what is being done with the system
- Paul <paul.walker@jamesmartin.com>

Singapore exchange blames outage on network failure

The Stock Exchange of Singapore [<http://www.ses.com.sg>] announced late Tuesday that the systems outage that left traders unable to complete any orders on Monday morning was caused by the failure of a communications link. The exchange said they became aware of the trading system failure at 8:10am on Monday and discovered the system was quickly shutting down every time it was restarted. After system checks revealed no problems, the exchange decided to switch to back up data from late Friday and then discovered a back up process at the Business Recovery Centre was still running. A Friday evening test on a communications link between the exchange and center had left the link down and this had kept the back up process running, explained the exchange in a statement. In an attempt to reassure investors, the exchange said "the trading system is sound," and announced "stringent procedures are being implemented to detect any failure to shutdown the systems properly. Checks are being put in place to ensure complete deactivation of systems before the commencement of any test." "With these measures, the problem should not recur," said the exchange.

eBay outage traced to failure to upgrade

"Steve Klein" <klein@dcds.edu>
Mon, 21 Jun 1999 16:30:13 -0400

This is supposedly a true story from a recent Defence Science Lectures Series, as related by the head of the Australian DSTO's Land Operations/Simulation division.

They've been working on some really nifty virtual reality simulators, the case in point being to incorporate Armed Reconnaissance Helicopters into exercises (from the data fusion point of view). Most of the people they employ on this sort of thing are ex- (or future) computer game programmers. Anyway, as part of the reality parameters, they include things like trees and animals. For the Australian simulation they included kangaroos. In particular, they had to model kangaroo movements and reactions to helicopters (since hordes of disturbed kangaroos might well give away a helicopter's position).

Being good programmers, they just stole some code (which was originally used to model infantry detachments reactions under the same stimuli), and changed the mapped icon, the speed parameters, etc. The first time they've gone to demonstrate this to some visiting Americans, the hotshot pilots have decided to get "down and dirty" with the virtual kangaroos. So, they buzz them, and watch them scatter. The visiting Americans nod appreciatively... then gape as the kangaroos duck around a hill, and launch about two dozen Stinger missiles at the hapless helicopter. Programmers look rather embarrassed at forgetting to remove *that* part of the infantry coding... and Americans leave muttering comments about not wanting to mess with the Aussie

wildlife...

As an addendum, simulator pilots from that point onwards avoided kangaroos like the plague, just like they were meant to do in the first place...

[Also noted by Scott Rainey. PGN]

✂ Faulty vending machines block emergency calls in Australia

"Nottingham, Mark (Australia)" <mark_nottingham@exchange.au.ml.com>

Mon, 5 Jul 1999 10:09:42 +1000

<<http://www.techserver.com/noframes/story/0,2294,66895-105845-751208-0,00.html>>

The default phone number in vending machines in Sydney is 000, which just happens to be the emergency phone number (a la 911 in the U.S.). As a result, hundreds of calls were made to emergency phone lines, blocking genuine calls. Authorities were trying to figure out how many of the million bogus calls a year are related to this source. [Source: AP item, 3 July; PGN-ed; also noted my others.]

✂ Brazilian telephone network chaos

"Matthew Todd" <matthew@mail.cmb.ac.lk>

Tue, 6 Jul 1999 10:08:26 +0600

I heard a report on the BBC World Service news this morning, 6 July, that only 15% of long distance telephone calls made in Brazil

yesterday were connected correctly. Apparently, a new dialing system was introduced over the weekend, which means people must now dial two extra digits. Residential customers have been asked not to make long distance calls during working hours for the next few days.

Matthew Todd, Lecturer in Computer Science, University of Colombo

⚡ **Spell-checker run amok? Shandling-->Changeling**

Jim Griffith <griffith@netcom.com>
Fri, 2 Jul 1999 14:57:06 -0700 (PDT)

CNN recently put a story on their entertainment page about a lawsuit which Garry Shandling filed against his former manager. However, other than the title, Shandling's name was changed throughout the article to "Changeling".
Can you say "spell-checker"?

<http://www.cnn.com/SHOWBIZ/News/9907/02/showbuzz/index.html#story1>

Jim

⚡ **REVIEW: "Computer Security", Dieter Gollmann**

Rob Slade <rslade@sprint.ca>
Mon, 21 Jun 1999 08:34:41 -0700 (PDT)

BKCOMPSC.RVW 990430

"Computer Security", Dieter Gollmann, 1999, 0-471-97844-2
%A Dieter Gollmann
%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8
%D 1999
%G 0-471-97844-2
%I John Wiley & Sons, Inc.
%O 416-236-4433 fax: 416-236-4448 rlangloi@wiley.com
%P 320 p.
%T "Computer Security"

Gollmann is fairly explicit in stating the intention and audience for the book. It is to be a text for a course, rather than a handbook, encyclopedia, or history. It is about computer security, rather than information security in general, although there are sections on computer network security and database security. The objective of the course for which it was prepared is to give students a sufficient background to evaluate security products, rather than to address issues of policy or risk analysis. Thus the emphasis is on technical, rather than managerial, aspects.

Part one lays the basic foundation for computer security. Chapter one outlines the fundamental vocabulary and concepts. Authentication is reviewed in chapter two. Examples from both UNIX and NT are used, in chapter three, to explain access control. Chapter four's discussion of security models requires a significant background in set theory, but for a course this can be assumed as a prerequisite. Considerations for hardware or operating system level security are looked at in chapter five.

Part two examines security in the real world. Chapter six provides a good review of the UNIX security functions. Security aspects of

NT

are described in chapter seven, but the effective interaction of rights and permissions is not clear (a failing shared by most NT security texts). A variety of ways in which security has failed are detailed in chapter eight. This concludes with a section on computer viruses in quite different format and level of detail. The reason for this is not made clear, but I am willing to grant that most security texts do not treat the subject as well. Chapter nine talks about the evaluation of security products, but concentrates on the formal criteria laid down by governmental agencies.

Part three looks at distributed systems. Chapter ten reviews specific systems, such as Kerberos and CORBA (Common Object Request Broker Architecture) security. Specific known Web vulnerabilities are effectively used to illustrate classes of threats in chapter eleven.

The explanation of cryptography in chapter twelve is nicely balanced for mechanics; a full description without a morass of detail; but is somewhat weaker on key management and cryptographic strength.

Network security, in chapter thirteen, deals with implementation level topics such as the IPsec (Internet Protocol Security) protocols and firewalls.

Part four deals with other aspects of security theory, primarily related to databases. Chapter fourteen and fifteen, respectively, discuss basic and advanced database security concepts. Problems of concurrent access, with applications in transaction processing, are examined in chapter sixteen. Security concerns of the object-oriented paradigm are raised in chapter seventeen.

In terms of readability, Gollmann's writing is not always fluid, but it is always clear. While intended as a class text, the book is, in most parts, accessible to any intelligent reader. The exercises provided at the end of each chapter are not mere buzzword tests, although most are more suitable for discussion starters than checks for understanding.

The bibliography is not annotated, but the "Further Reading" section at the end of each chapter helps make up for this shortcoming. Having to flip between two sections to find the referenced work is a bit awkward, but not unduly so.

This is a very welcome addition to the general computer security bookshelf.

copyright Robert M. Slade, 1999 BKCOMPSC.RVW 990430
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

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

🔥 REVIEW: "Securing Java", Gary McGraw/Edward W. Felten

"Rob Slade" <rslade@sprint.ca>
Tue, 22 Jun 1999 08:37:10 -0800

BKSECJAV.RVW 990501

"Securing Java", Gary McGraw/Edward W. Felten, 1999, 0-471-31952-X,

U\$34.99/C\$54.50

%A Gary McGraw gem@rstcorp.com

%A Edward W. Felten felten@cs.princeton.edu

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8
%D 1999
%G 0-471-31952-X
%I John Wiley & Sons, Inc.
%O US\$34.99/C\$54.50 416-236-4433 fax: 416-236-4448
rlangloi@wiley.com
%P 324 p.
%T "Securing Java: Getting Down to Business with Mobile Code"

Unlike Oaks "Java Security" (cf. BKJAVASC.RVW), this book concentrates on Java in the popular perception: as a means of providing active code on the Web. As such it is intended not simply for techies, but also for dedicated users.

Chapter one provides a readily accessible backgrounder, covering portability, the Internet, the Web, active content, security risks, other active content systems, and a rough outline of the Java security model with particular regard to applets. The original Java applet security model, or "sandbox," is covered in chapter two. The security model is now complicated by signed code, and chapter three points out the changes made. Chapter four outlines a number of malicious applets, but also gives clear directions for disabling Java on both the Netscape and Internet Explorer browsers. The authors outline a second class of hostile applets, in chapter five, that are intended to breach system security and allow an attack to bypass normal security mechanisms. There are suggestions for improving the security model, as well as a review of third party attempts to enhance it, in chapter six. (I was amused to see the slight lifting of the skirts of ICISA

[International Computer Security Association]: the history of the outfit is a lot more interesting and convoluted even than is portrayed here.) Chapter seven is directed at programmers, but the advice provided looks at practices and policies rather than APIs (Applications Programming Interfaces) and chunks of sample code. A version of Java specifically designed for Smart Cards is available, and chapter eight looks at its promises and problems. A recap and restatement of the major security issues in mobile code is given in chapter nine. Appendices provide a Java security FAQ, security resource pointers, and directions on Java code signing.

The text is quite readable. The authors have made a very serious attempt to ensure that the book does not depend upon previous technical background. For the most part, they have succeeded. The diligent reader would be able to understand most of the concepts as presented, even without having worked with computers or computer security. However, the key word is "diligent:" it *feels* like a technical book, and newcomers to the topic may be put off by the style.

In addition, McGraw and Felten are careful to avoid any bias. They obviously feel that Java has some worthwhile security measures, but admit to its faults and point out its shortcomings. This makes the book extremely useful: much more so than an uncritical paean of praise.

An effective book on an important subject with a wide audience. But you don't have to take my word for it. You can try before you buy. The www.securingjava.com site does not simply contain a few press releases and the errata, but has the whole text of the book online. A

bold step. (You can help justify it by then buying the book.)

copyright Robert M. Slade, 1999 BKSECJAV.RVW 990501
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

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



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 48

Thursday 15 July 1999

Contents

- [London Underground sequence rollover](#)
[Lloyd Wood](#)
- [Software disaster leaves new Australian submarine unfit](#)
[Quentin David Jones](#)
- [Computer glitch causes severe train delays in Melbourne](#)
[Stuart Lamble](#)
- [Medical paper retracted following discovery of programming error](#)
[John Doyle](#)
- [Life-threatening flaw in implantable cardioverter-defibrillator](#)
[John Doyle](#)
- [Potentially life-threatening medical equipment failure](#)
[John Doyle](#)
- [Toyota smog-warning computer suit](#)
[Taz Daughtrey](#)
- [Financial Engines: Should I jump off the bridge or live it up?](#)
[Susan Gerhart](#)
- [Cancelling errors, serendipity in avoiding risks, and Kepler](#)
[Henry Baker](#)
- [Traffic signals going all-green](#)
[Jeff and Glenn Grigg](#)

- [Privacy statement risk, quoted without comment](#)
[Andrew Koenig](#)
 - [Re: Garciaparricide in All-Star balloting?](#)
[David Cassell](#)
 - [Re: Space Station AOL hack](#)
[Leonard Erickson](#)
 - [Re: Electronics startup transient kills spacecraft](#)
[Fernando Pereira](#)
 - [Re: E-mail writer arrested for starting panic](#)
[Cameron Hayne](#)
[J.D. Abolins](#)
[John O'Connor](#)
 - [Webmail is not the same as anonymous e-mail](#)
[Scott A Crosby](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ London Underground sequence rollover

Lloyd Wood <L.Wood@surrey.ac.uk>
Sat, 10 Jul 1999 16:49:15 +0100 (BST)

Surprise! London Underground Travelcards that are at least 2 years old just happen to work. As a result, the cards are being sold on the black market for over 50 pounds for four-zone cards. The mag stripe information format just happens to match, giving unlimited free rides. However, not of the all old cards work. Estimates of fare fraud already exceed 25 million pounds a year, just over 3 million of which is offset by 10-pound fines for misuse.

[Source: Touts cash in on old Tube Travelcards, by Dick Murray, Transport

Editor, London *Evening Standard*

<http://www.yahoo.co.uk/headlines/19990709/london/newsstory154274.html>]

[As usual, the suggested fix is to completely replace the system -- with a new smart-card system. Interesting that the cards aren't specifically tied to the calendar date, which would have prevented this. Risks lie in costs of manual checks to safeguard the intent of the system... Lloyd.]

<L.Wood@surrey.ac.uk>PGP<<http://www.ee.surrey.ac.uk/Personal/L.Wood/>>

🔥 Software disaster leaves new Australian submarine unfit

"Quentin David Jones" <quentinj@opera.iinet.net.au>
Mon, 5 Jul 1999 06:53:19 +0800

The latest (and independent) report to the Australian Gov. concerning the problems with its new Collins class submarine project recommends the entire combat system be scrapped and replaced with a new off-the-shelf system (at a cost of hundreds of millions).

The McIntosh-Prescott report, released 1 Jul 1999, also notes other major problems with the new submarines, including unreliable diesel engines, excessive noise, cracking propellers, poor communications and periscope vision. Deficiencies in project management and procurement were also criticised.

The hardware issues, though serious, can be fixed -- but the software for the combat system is considered unlikely to ever work. Currently

Boeing is working on an interim fix which is described as a "short-term band-aid" which should provide some quick improvements, but which will not lead to a satisfactory solution. We also have an urgent joint US/Aus. Navy project which will spend \$A 80 million to help rectify some of the key software problems inter alia.

The major conclusion of the report however, is to completely dump the software and start again - "A preferred new system would be configured with less-integrated architecture and would utilise more off-the-shelf equipment".

Note the comment "less-integrated".

The plans for the combat system called for a tightly integrated system which instead of having dedicated stations for specific tasks (i. e. a sonar station, a separate torpedo control station, comms station, etc.), would have 7 general purpose workstations which could each be configured to perform any (or all) tasks as required. At the time this ambitious plan was rightly criticised.

Fears of cost over-runs led to an insistence on a fixed-price contract originally signed in 1987. Computer technology advanced significantly during the life of the project, so that many components were out-of-date by the time they came into use.

It appears that the top brass failed to respond quickly enough to many warning bells about the combat system.

The result is that Australia has only 1 obsolete submarine in service, and if the problems on the Collins are not fixed quickly, may end up with no working submarines at all for some time.

Quentin David Jones

🔥 Computer glitch causes severe train delays in Melbourne

<slamble@csc.com>

Mon, 12 Jul 1999 11:22:22 +1000

On 8 July 1999, a glitch in a computer system caused train signals in the area around Flinders Street Station (a major station in the central business district of Melbourne, Australia) to fail. The glitch occurred at 5:40pm, and was not rectified until 6:20pm -- right in the middle of peak hour. The congestion was not completely cleared until 7pm, and even then, trains were running up to two hours behind schedule. The glitch affected trains traveling to and from the south-eastern and eastern suburbs (definitely Lilydale, Belgrave, Glen Waverley, and Alamein lines; also the Hurstbridge and Epping lines, according to the local tabloid). In addition, trains traveling through the underground city loop to northern and western suburbs had to be re-routed to travel direct, bypassing the loop.

There have, apparently, been other similar glitches in the past, lasting for up to five minutes; this is (to the best of my knowledge) the first

lengthy delay, certainly in the middle of peak hour. Speaking as somebody who was caught in a train for half an hour between Richmond and East Richmond, I have to say that I've discovered a new swear word: "Public Transport". :-)

Standard RISK: all the eggs in one basket, with no backup (electronic _or_ manual) in place.

Time to move closer to work and start using my bicycle, I think.

✶ Medical paper retracted following discovery of programming error

"Dr D John Doyle" <djdoyle@home.com>
Sat, 10 Jul 1999 12:37:24 -0400

The 14 Jan 1999 issue of the **New England Journal of Medicine** (arguably the most prestigious medical journal published) contained an unusual retraction. This time at issue was not the discovery of fraudulent research, a nasty problem afflicting top medical journals for some time now, but the discovery of a computer programming error in a study of suicide rates following natural disasters. The mistake resulted in the software erroneously counting some deaths twice.

When the data was restudied following the correction of the error, the conclusion of the original paper was found to be incorrect. The authors acted ethically in reporting this error and retracting their paper, despite the embarrassment and career implications involved. How many

others would have merely kept quiet and not issued a retraction, especially knowing that failure to weed out this misinformation would not likely result in any patient harm (as compared to, say, an error in a dose-finding study)?

This problem also raises the issue of the role of senior clinical investigators, most with very limited programming skills, in supervising the efforts of the programmers that work on their research team.

REFERENCE: Krug EG, Kresnow M, Peddicord JP, Dahlberg LL, Powell KE, Crosby AE, Annest JL Retraction of "Krug EG, Kresnow M, Peddicord JP, Dahlberg LL, Powell KE, Crosby AE, Annest JL. Suicide after natural disasters. N Engl J Med 1998 Feb 5;338(6):373-8 " N Engl J Med 1999 Jan 14;340(2):148-9

D. John Doyle MD PhD, Associate Professor, University of Toronto
djdoyle@home.com

⚡ Life-threatening flaw in implantable cardioverter-defibrillator

"John Doyle" <djdoyle@hotmail.com>

Sat, 10 Jul 1999 17:10:18 PDT

A recent report in a medical journal describes a life-threatening event in a 70-year old man in whom an implantable cardioverter-defibrillator had been previously placed to regulate the patient's erratic heartbeat following a previous cardiac arrest. Unfortunately, a software malfunction in the unit later occurred such that the patient developed an "acute onset of dizziness"

from "loss of ventricular output due to an internal software problem". The problem was corrected by reprogramming the unit via the external programmer.

REFERENCE: Coppess MA, Miller JM, Zipes DP, Groh WJ Software error resulting in malfunction of an implantable cardioverter defibrillator. J Cardiovasc. Electrophysiol. 1999 Jun;10(6):871-3

D. John Doyle MD PhD, Associate Professor, University of Toronto
djoydo@home.com

✦ Potentially life-threatening medical equipment failure

"John Doyle" <djoydo@hotmail.com>

Sat, 10 Jul 1999 17:53:07 PDT

Patient monitors are used extensively in acute care medicine, especially during surgical procedures or when transporting critically ill patients. In an interesting report by two anesthesiologists a potentially life-threatening situation is described whereby a transport monitor provided data that did not seem to match the doctors' clinical assessment of the patient. Among other things, the digital pressure display never varied from 120/70. Suspicious that something was wrong, the doctors rechecked everything only to find that on close inspection of the fine print on the transport monitor's screen the words "demo mode" appeared intermittently. They then realized that all of the waveforms and data on the screen were simulated! Even worse, attempts to turn off the "demo mode"

failed because a password is needed both to enter and to leave the simulation mode! The doctors switched to another monitor. No harm came to the patient.

An investigation later revealed that "the hospital biomedical engineer had used the internal password to place the monitor into the simulation mode for testing, but had neglected to return it to normal patient monitoring mode before certifying it as fit for clinical use."

The following comments from the authors are worth heeding: "Anesthesiologists should be aware of this novel form of monitoring "failure." . . . Obviously, human failures were involved in this incident, but improved equipment design could have helped prevent our patient from being exposed to the risk of not being monitored. In particular, we believe it is inappropriate for a password to be needed to exit from an internal simulation mode. We also recommend that manufacturers make "demo mode" messages more obvious when a monitor is in a simulation mode by appropriate use of text size, color, and/or brightness and by having it flash. Such messages should be present continuously, not intermittently. A high state of vigilance continues to be warranted, particularly around the time of patient transport."

REFERENCE: Ramundo GB, Larach DR. A monitor with a mind of its own. *Anesthesiology* 1995 Jan;82(1):317-8

D. John Doyle MD PhD, Associate Professor, University of Toronto
djoydoyle@home.com

⚡ Toyota smog-warning computer suit

<Sqpeditor@aol.com>

Mon, 12 Jul 1999 22:22:11 EDT

The Justice Department has filed a civil suit under the Clean Air Act (on behalf of the EPA) against Toyota for faulty smog-control computers on 2.2 million 1996-1998 vehicles (Camry, Avalon, Corolla, Tercel, Paseo; Lexus; Sienna minivans, etc.). The suit seeks repairs and fines up to \$58.5 billion for faulty software that failed to detect above-threshold emissions. California had apparently approved the systems based only on simulations. Toyota claims the rules were altered after the initial approvals. [AP item, 12 Jul 1999, PGN-ed]

Taz Daughtrey, SOFTWARE QUALITY PROFESSIONAL, SQP_Editor@asqnet.org

⚡ Financial Engines: Should I jump off the bridge or live it up?

Susan Gerhart <slger@mindspring.com>

Wed, 14 Jul 1999 15:12:16 GMT

Many financial planning articles, including a recent Jane B. Quinn Newsweek column, tout a new retirement planning service at <http://www.financialengines.com>. This operation uses risk-driven models from co-founder Bill Sharpe, a Nobel Laureate, and is strongly VC funded. Incorporating risk gives a probability of certain annual income with

ranges and "what-if" scenarios for various portfolio allocations. The on-line implementation is a Java applet with portfolio data held and updated on their server.

I put in my approximate data and ran the forecast. Amazingly, no matter how *high* I cranked the annual income goal, e.g. \$200K, the result was >95% sunny (literally) forecast. Not real, I was sure, so I ran it on another PC. Same data, held on their site, but this time no matter how *low* the annual goal, e.g. \$5K, the applet always gave <5%, very stormy, forecast. In other words, complete opposite results depending upon PC (MICRON pentium-I was more optimistic than Gateway Pentium-II, independent of browser). FinancialEngines tech support responded quickly to the problem and in a few days the schizophrenic forecasts settled down, apparently fixed and downloaded. I'm still hoping for a technical explanation but haven't heard from customer support.

Clearly the program didn't have any built-in guards against ridiculous answers. Some people using the model might be blissfully overspending and others suicidal depending upon their Java/Pentium interaction. But most users of these planners know they have to try several, examine assumptions and models carefully, and pray.

Even well-funded Nobel Laureates have QA problems.

susan gerhart

✶ Cancelling errors, serendipity in avoiding risks, and Kepler

Henry Baker <hbaker@netcom.com>

Mon, 12 Jul 1999 16:28:39 -0700

Subtitle:

Serendipity = Error2 - Error1 ? (or
Serendipity = [Error1,Error2] using commutators!)

RISKS spends a lot of time bemoaning the negative side of errors. Perhaps more time should be given to "serendipity" which I loosely translate as "order from chaos". Serendipity is celebrated by authors and film-makers as the way to find love after some disastrous mistake. But science also proceeds in such ways.

A famous example is that of Kepler. I quote from "Fundamentals of Astrodynamics" by Roger Bate, Donald Mueller, and Jerry White, 1971, Dover ISBN 0-486-60061-0 (Sec 4.1, p. 178):

"Kepler's first task was to determine the radius of the circle [of the orbit] and the direction of the axis connecting the perihelion and aphelion. At the beginning of a whole chapter of excruciating trial-and-error calculations, Kepler absentmindedly put down three erroneous figures for three vital longitudes of Mars, never noticing his error. His results, however, were nearly correct because of several mistakes of simple arithmetic committed later in the chapter which happened very nearly to cancel out his earlier errors.

"At the end he seemed to have achieved his goal of

representing within 2

arc-minutes the position of Mars at all 10 oppositions recorded by Tycho.

But then without a word of transition, in the next two chapters Kepler

explains, almost with masochistic delight, how two other observations from

Tycho's collection did not fit: there was a discrepancy of 8 minutes of

arc. Others might have shrugged off this minor discrepancy between fact

and hypothesis [or fudged his numbers a la Newton's Moon]. It is to

Kepler's everlasting credit that he made it the basis for a complete

reformulation of astronomy. He decided that the sacred concept of

circular motion had to go. [...]

"Forgetting his earlier resolve to abandon circular motion he reasoned,

again incorrectly, that, since speed was inversely proportional to

distance, the line joining the sun (which was off-center in the circle)

and the planet swept out equal areas in the orbit in equal times.

This was his famous Second Law--discovered before the First--a law of

amazing simplicity, arrived at by a series of faulty steps which he

himself later recognized with the observation: 'But these two errors--it is

like a miracle--cancel out in the most precise manner, as I shall prove

further down.'

The correct result is even more miraculous than Kepler realized since his

explanation of why the errors cancelled was also erroneous!"

The search for the source of errors is often times hugely more

valuable than
the original error. The progress of science is pretty much
fueled by
errors. How many times have you searched for a minor bug and in
the process
of correcting it fixed a major bug? (I seem to recall that
David Moon, ex
of Symbolics and Apple, used to call these "dead bears",
probably having
something to do with letting sleeping and/or dead bears alone.)

Henry Baker

⚡ Traffic signals going all-green

Jeff Grigg <jeff@michelob.wustl.edu>

Tue, 13 Jul 1999 09:04:32 -0500

I noted the old RISKS postings in the archive about traffic
signals going
"all green," allowing conflicting traffic:

[RISKS-18.94:](#)

Traffic signals, red-runners & all-greens (J. DeBert)

[RISKS-18.95:](#)

Re: all-ways green lights (Robert Miller, Sean Ercanbrack,
Barak Pearlmutter)

[RISKS-19.01:](#)

Re: all-ways green lights (Mark Brader, Steve Summit, Dik T.
Winter)

[RISKS-19.03:](#)

All-ways green lights ... it's all in the timing (Richard Cook)

So, I thought to ask my uncle, a recently retired traffic
consultant living
in the San Francisco area. This is his response:

From: Glenn Grigg [SMTP:glennmg@juno.com]

Date: 25 June 1999

Subject: Re: "all-green" on traffic lights

First of all let me tell you, after a collision at an intersection, [...] they ALL say [they had a green light]! Now, lets talk chips and software. The modern traffic signal controller IS software driven, however, they are rather simple machines with "if this, do that, but not the other" kinds of decisions to make. Bugs? Maybe, but I've never seen conflicting greens due to controller software! I have seen wires get crossed, like when someone knocks a signal pole down and the insulation on the wires get stripped.

NOW, let me tell you about the conflict monitor. This is a device that is connected to the field wires at the terminals where the 110v AC wires go from the cabinet directly to the light bulbs that illuminate the signal faces. This device does NOT monitor the controller or its software, it monitors the 110v AC lines. If a software bug were to direct the load switches close and send 110v AC to green signal faces that face conflicting traffic, this monitor would detect this conflict and put the intersection on flash. Do conflict monitors fail? Are they made by Humans? That's why we test our conflict monitors on a regular basis. Well, how do we do this? The sophisticated way is to bring it in the shop and hook it up to a special monitor tester. However, there is a simple way to do this in the field. You take a short piece of wire, preferably insulated, and you stick one end in the 110v AC terminal of any green indication wire. With the other end, you

stick it to any other green indication terminal. You have 110v AC in your hands, that's why I use an insulated wire. When you stick it on a conflicting green terminal the monitor will "trip" and the intersection will go immediately to flashing. DON'T do this during the rush hour! You'll be getting off lightly if people only curse at you!

Glenn

⚡ Privacy statement risk, quoted without comment

Andrew Koenig <ark@research.att.com>
Tue, 13 Jul 1999 15:44:25 -0400 (EDT)

From a website's privacy statement:

Children 12 years of age and younger are not permitted to opt in for these future e-mailings because the opt-in software requires users to fill in their age and only users above 12 years of age are able to submit opt-in authorizations.

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

⚡ Re: Garciaparricide in All-Star balloting? ([RISKS-20.47](#))

David Cassell <cassell@mercury.cor.epa.gov>
Sat, 10 Jul 1999 15:03:45 -0700

The Chris Nandor who deluged the All-Star ballot site with 22,000-some votes

for the Red Sox shortstop is not only a huge Red Sox fan [no kidding - his e-mail handle is 'pudge' for Carlton Fisk], but also a known Perlite. He is the Chris Nandor who co-wrote "MacPerl: Power and Ease" with Vicki Brown.

He merely used the LWP::Simple module with a few lines of Perl code to produce his anti-Jeter machine. He clearly didn't try to obscure his identity. It would have been trivial for him to spoof his e-mail address, as well as generating random valid numbers for phone number and zip code.

Given this thought, one has to wonder how many people actually made the effort to conceal the fact that they were making multiple votes. I see a major-league RISK just around the corner for the All-Star voting site. What happens when someone makes the effort mentioned above and dumps 500,000 votes in on the last day to get their favorite player(s) in?

In 1957, the Cincy fans did such a good job of ballot-stuffing that the commissioner had to step in and hand-select other players to start. The names of some of the players who had been pushed out? Oh, no one big, just Musial, Aaron, Mays, ... Now it will only take one person and a 40-line Perl script to do the same thing.

David Cassell, OAO cassell@mail.cor.epa.gov
Senior computing specialist, mathematical statistician

✶ Re: Space Station AOL hack (Passy, [RISKS-20.47](#))

Leonard Erickson <shadow@krypton.rain.com>

Sun, 11 Jul 1999 00:02:36 PST

> Similar to problems AOL has had, it seems that someone, most likely
> someone involved with the ISS program, obtained the name of a user with
> administrator access, then called the help desk and asked for a password
> reset. They were promptly given that new password, after which they
> proceeded to do something objectionable with the password file. (That
> part's still not quite been released.)

Argggh!

I know I'm preaching to the choir here, but when I've been administering a system, the policy was that to get a new password, you did one of three things:

1. Show up at my desk and have my hand you the new password.
2. Call me **directly**. This was **only** allowed for people I could recognize over the phone.
3. Call or e-mail me, and the new password would go out via internal **physical** mail sealed inside a use once envelope with CONFIDENTIAL on it in large letters.

At one time we allowed people to informally request accounts & passwords for people working under them. This was stopped after someone slipped in a request for an account for "John Tuttle" (M*A*S*H reference) into the system. They then posted some inappropriate messages to the internal e-mail system.

After that, we went **strictly** formal on new account requests.

> [... PIN for resets ...]

Yeah. Some folks just don't get it. :-)

Leonard Erickson (aka Shadow) shadow@krypton.rain.com

⚡ Re: Electronics startup transient kills spacecraft ([RISKS-20.47](#))

Fernando Pereira <pereira@research.att.com>

Sat, 10 Jul 1999 20:16:18 -0400

> [...] leaving the circuit in a non-deterministic state [...]

A question for those who know about such things: is current education in digital circuit design sufficiently attuned to the subtleties of the physical world, or do students have an overly simplistic view of how bits are represented in hardware? Given the deterioration of continuous math education in high school and universities, I wonder...

⚡ Re: E-mail writer arrested for starting panic ([RISKS-20.47](#))

"Cameron Hayne" <hayne@crim.ca>

Sat, 10 Jul 1999 14:23:03 -0400

> 2. Since Hotmail accounts are notoriously anonymous, how was this tracked

> back to him so that he could be arrested?

> [Anonymity is generally only a relative concept. Who pays the bills? PGN]

You don't seem to know that Hotmail accounts are free, hence truly anonymous.

Cameron Hayne (hayne@crim.ca), Centre de recherche informatique de Montreal

✂ Re: E-mail writer arrested for starting panic (Todd, [RISKS-20.47](#))

"J.D. Abolins" <jda-ir@njcc.com>
Sat, 10 Jul 1999 17:05:10 -0700 (PDT)

Couple of comments regarding this interesting item...

1. Hotmail and many other Web-based e-mail accounts aren't really anonymous.

They can be pseudonymous in that the user can choose whatever handle and registration info he may want. It is not unique. There are other Internet access resources where identity is not particularly verified. Sounds like end of all accountability but it isn't. There are still many clues available if an incident draws enough attention.

2. Many Web-based e-mail services do give some useful clues in their e-mail's headers. The most useful is the IP address of the system from which the e-mail was submitted via HTTP. I have used this to trace a series of e-mail harassment using Hotmail.com. A form of whois lookup can provide the info for who has the set of IP addresses that include the one listed in the header. The owner of the IP address can be contacted and they can use their

logs to find out whose account was used. That is probably what happened in this e-mail panic case.

J.D. Abolins

✶ Re: E-mail writer arrested for starting panic (Todd, [RISKS-20.47](#))

"John O'Connor" <jp0c@hotmail.com>

Mon, 12 Jul 1999 02:43:33 PDT

Every e-mail sent out from the hotmail system carries, in the e-mail headers, the IP address of the machine hosting the web browser used to compose the message.

This is another risk, isn't it. The risk of assuming that a system is anonymous just because it is notoriously anonymous. :-)

Get Your Private, Free E-Mail at <http://www.hotmail.com>

✶ Webmail is not the same as anonymous e-mail.

Scott A Crosby <crosby@qwes.math.cmu.edu>

Sun, 11 Jul 1999 00:48:25 -0400 (EDT)

I've been using a trick to identify abusers who used hotmail already. And the recent Risks article: 'E-mail writer arrested for starting panic' showed that this trick isn't as well known as I thought.

Many webmail providers I have seen tend to introduce interesting headers

into e-mail sent by them. For example, hotmail appends the following header to outgoing e-mail. Past this, identification is trivial.

```
X-Originating-IP: [206.47.244.30]
```

Regardless of whether or not the webmail provider actually appends such a header, they are very likely to log e-mails anyways. Thus it is very easy for legal or political pressure to grab the logs and identify the user.

So perhaps the risk here is that people have been thinking that webmail means anonymous e-mail.. It doesn't.

The most reliable way I can find to truly send e-mail anonymously is through the anonymous e-mailer network. (Or maybe a mixmaster network).

If you wish to also get responses anonymously, supply a reply-block that sends responses through a web-forwarder service dumping into a webmail dropbox. Then access the dropbox through onion-routing.

Scott



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 49

Wednesday 21 July 1999

Contents

- [Intercom hang-up caused 1997 train collision](#)
[Mark Brader](#)
- [Computer-based patient monitor problems: improvements still needed](#)
[John Doyle](#)
- [Statistical errors in medicine](#)
[John Doyle](#)
- [Centaur/Milstar Software Error](#)
[Peter B. Ladkin](#)
- [Small problem escalates into major disruption](#)
[Doug Moore](#)
- [Computer startup circuits](#)
[M. Simon](#)
- [Netcom partial e-mail outage](#)
[Keith A Rhodes](#)
- [junkfilter vs. xxx.lanl.gov](#)
[Thomas Roessler](#)
- ["Bright Light" POP-based spam filtering: a bad idea](#)
[Lauren Weinstein](#)
- [E-mail attachments and local names](#)
[Avi Rubin](#)

- [Ab van Poortvliet: Risks, Disasters, and Management](#)
[PGN](#)
 - [REVIEW: "The Mythical Man-Month", Frederick P. Brooks Jr.](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Intercom hang-up caused 1997 train collision

<msbrader@interlog.com>

Fri, 16 Jul 1999 00:40:38 -0400 (EDT)

On November 19, 1997, two GO commuter trains collided at low speed in Toronto's central station (Union Station). One was stationary, with 800+ people on board, of whom 50+ were injured enough to be taken to hospital; the other would have been the next train out of the same track, and only two crew members were aboard.

<<http://www.bst-tsb.gc.ca/eng/reports/rail/1997/er97t0299.html>>

is the official report, and two things it discusses seem worth a write-up here.

The first is the "dwarf signals" used for shunting moves in the station area, where it's not uncommon for trains to be sent onto an already-occupied track.

When a move was authorized, the dwarf signal would show green (15 mph okay)

if the track was actually clear AND the movement was in the preferred

direction for that track, but otherwise yellow (15 mph max, but must be

able to stop within half the distance you can see).

This is all right if everyone drives according to the rules, but it means

that yellow sometimes does and sometimes doesn't mean that there's a train known to be on the track. And a survey of train crews after the accident revealed that they generally did not know this.

The second and I think more serious problem was the intercom. Commuter trains with diesel locomotives often have the locomotive permanently at one end, and a driving cab in the car at the other end, allowing quick reversal between trips, and that's what GO does. On this occasion the train was making a short reverse move to change tracks, and the engineer (driver) elected to stay in the locomotive and drive from the rear for the second move. The conductor was to keep a lookout ahead from the cab car.

Now, there is a good deal of train radio traffic in the area, and GO trains have an intercom between the two cabs, so the crew members naturally used that instead of their radios. To start a conversation they would have to buzz the other cab for attention and wait for the other person to pick up the handset. The risk factor is that there was NO indication of when the handset had been HUNG UP again -- and no official rules for intercoms, which could have required someone to say when they were hanging up.

The conductor had been on the intercom a little before he sighted the other train, which was still a safe 200 feet away, and he assumed the engineer was still listening -- so when called for a stop, he didn't buzz first! And then when he realized that the train wasn't braking, he didn't have

quite enough time left to correctly decide what it was best to try next.

Mark Brader, Toronto msbrader@interlog.com

⚡ Computer-based patient monitor problems: improvements still needed

"Dr D John Doyle" <djdoyle@home.com>

Sat, 17 Jul 1999 14:46:39 -0400

As an anesthesiologist with 30 years of computer experience I sometimes give thought to the design of the computer-based instrumentation on which my patients lives depend. For example, when I put a patient to sleep for heart surgery, I insert monitoring lines to follow cardiac filling pressures, cardiac output pressures and other parameters such as the electrical pacing and conduction properties of the heart. Usually five or more signals are displayed in real-time on a high-resolution display. This data is just as important to us as flight-related data is to an aircraft pilot, and forms the basis on deciding, for example, which drugs we administer to get out of clinical crises.

Regretfully, personal clinical experience has lead me to realize that much needs to be done to make patient monitors trustworthy and ergonomically sensible. Two examples illustrate the point.

I know of two computer-based monitor designs that occasionally "reboot" in the middle of surgery for no apparent reason (possibly due to

electromagnetic interference from the electrosurgical apparatus, or even nearby cellular phones, but possibly also software-related), with the result that the patient is at increased risk during the reboot period (where you are "flying blind"). The situation is especially frustrating when the pressure-signal-related zero offset information is lost on reboot and the pressure transducers must all be rezeroed!

Also, another monitoring system I use frequently will annunciate an "asystole" (cardiac arrest) alarm when ever the electrocardiogram signal falls below a certain amplitude. The fact that normal cardiac pressures are still being generated is ignored by the alarm management software, resulting in an obviously wrong diagnosis. This kind of haphazard and ill-conceived alarm arrangement is the reason why many of my colleagues globally disable all alarms at the beginning of surgery, so they can concentrate on taking care of the patient rather than following up on countless false alarms.

So much needs to be done!

D. John Doyle MD PhD FRCPC, Associate Professor, Department of Anesthesia,
University of Toronto djdoyle@home.com <http://doyle.ibme.utorono.ca>

Statistical errors in medicine

"John Doyle" <djdoyle@hotmail.com>

Tue, 20 Jul 1999 10:52:22 PDT

Since physicians are not in general particularly inclined towards mathematics, some individuals have expressed concern that statistical or other analytical errors may sometimes creep into medical research reports as a result. It would appear that, in fact, this is truly a problem. Several studies of statistical errors present in medical journals have been undertaken by statistical experts; their results suggest that statistical errors are frequent in published medical research reports, even in "prestigious" journals such as The New England Journal of Medicine.

For example, in a British study [1] papers published in the British Journal of Psychiatry in 1993 were reviewed. Sixty-five (40% of 164) papers containing numerical results contained statistical errors. While many errors were not serious, some were viewed to be sufficiently problematic to cast doubt on the conclusions. The author concluded that the statistical error rate was "unacceptably high."

Similarly, in an American study [2] the authors reviewed all papers included in the Clinical Articles section and transactions of societies sections of the January through June 1994 issues of the American Journal of Obstetrics and Gynecology (volume 170, numbers 1 to 6). The authors concluded: "The lack of complete and detailed listings of applied statistics made it difficult to assess the appropriateness of more than half the studies

examined, suggesting a need for more detailed guidelines as to the listing of statistical procedures used. Despite this fact, nearly one third of the articles contained examples of statistics used inappropriately."

More recently, a study on the misuse of correlation and regression in three top-rated medical journals found serious problems [3]. The authors noted:

"Fifteen categories of errors were identified of which eight were important or common. These included: failure to define clearly the relevant sample number; the display of potentially misleading scatterplots; attachment of unwarranted importance to significance levels; and the omission of confidence intervals for correlation coefficients and around regression lines."

I suspect that one problem may be the availability of easy-to-use statistical software that makes no requirement that the user actually understand the underlying principles behind the tests employed. In any event, it would appear that the general standard of statistics in medical journals is shabby. Perhaps special emphasis should be given to the necessity for medical journals to have proper statistical refereeing of submitted papers. Indeed, some journals, embarrassed by reports such as these, are doing exactly that.

References

- [1] McGuigan SM The use of statistics in the British Journal of Psychiatry.
Br J Psychiatry 1995 Nov;167(5):683-8

[2] Welch GE 2nd, Gabbe SG Review of statistics usage in the American Journal of Obstetrics and Gynecology. Am J Obstet Gynecol 1996 Nov;175(5):1138-41

[3] Porter AM Misuse of correlation and regression in three medical journals. J R Soc Med 1999 Mar;92(3):123-8

D. John Doyle MD PhD, Department of Anesthesia, University of Toronto
djdoyle@home.com <http://doyle.ibm.utoronto.ca>

✶ Centaur/Milstar Software Error (Re: [RISKS-20.36](#) and 39)

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>
Tue, 22 Jun 1999 18:43:22 +0200

As reporting in [RISKS-20.36](#) (PGN) and [20.39](#) (Rhodes), software failed in a Centaur upper stage of a Titan IVB rocket, launched from Cape Canaveral on 30 Apr 1999, resulting in the loss of an \$800-million Milstar satellite.

Aviation Week (21 Jun 1999, p21) writes that Air Force officials said that the error was in the Centaur's attitude control system software. The inertial nav unit `perceived' a zero roll rate, which was incorrect, `creating attitude errors'. The attitude control system tried to correct attitude, but the incorrect software parameter `prevented the system from orienting the stage properly'. Attitude control system fuel ran out. The USAF and LM don't yet know how the software error escaped detection during

verification.

Let me try to interpret this. I'm afraid I won't do very well. All these control system bits, software or hardware, have inputs and outputs. An inertial nav unit (INU) calculates position only, using information from the dynamics history of the vehicle. To say it `perceived' a zero roll rate is to say either that something fed it zeros instead of correct information about roll, or that it gave information out about a roll rate of zero, or maybe both. To say that this `created attitude errors' is to say that the control system responsible for controlling the attitude (ACS) failed (`attitude errors'), and to subscribe this to faulty input from the INU (`created'). Since the ACS tried to `correct' this, it must mean that although the ACS was working on faulty information from the INU, it obtained other input (from somewhere else?) or calculated the information internally that contradicted this faulty information, and resolved the conflict in favor of this new information, firing the attitude control thrusters (I think that's what such things are called). But apparently the faulty info from the INU still exerted an influence (`incorrect .. parameter prevented the [ACS] from orienting the stage properly').

As far as I understand such things, when a sensor/info conflict is detected, a system will act on the conflict by attempting to identify (or, if not, simply arbitrate) the faulty information and lock it out. Or maybe, if it's really sophisticated, use Byzantine resolution techniques,

if ways have
been found of implementing these efficiently now. I don't know
of any system
design which, having identified a conflict, proceeds to use both
pieces of
conflicting information further, unless it's trying Byzantine
resolution
techniques, which require four participants at least. I don't
see the
four here, so this story, even though sparse, still doesn't make
sense to
me yet. And I'm loathe to ascribe truth to a story which doesn't
even make
sense. But I guess I'm grateful to AvWeek for trying.

Prof. Peter Ladkin, Univ. Bielefeld, Technische Fakultät D-
33501 Bielefeld
GERMANY +49 (0)521 106-5326/5325 <http://www.rvs.uni-bielefeld.de>

✶ Small problem escalates into major disruption

<dougmoore@ibm.net>

Sun, 18 Jul 1999 16:51:28 -0400

A very small fire at a major Bell switching centre caused at
least 113,000
phone lines to go out in Toronto's downtown business section,
including
lines to poison information centres and paramedics, and stopped
bank
machines, electronic credit card systems, Interac, many
computerized traffic
lights, nearly \$1 billion of electronic stock exchange trading,
and several
major data networks and internet portals, and disrupted phone
services as
far away as Ottawa, Halifax, and Chicago. 911 emergency lines
had reduced
capacity but did stay up. The fire was caused by a technician

dropping a rod in a single switching chamber; which started to fry or melt, and smoke filled the area and sprinklers went off. (Later reports say it was electric arcs, not fire.) Power in that one part of the building was lost --- putting some phones out of service. Employees were unable to get close to turn the power back on in that area. (There was no remote power switch to do it?) According to reports in the Toronto Star, the emergency power generator system was not designed to kick in unless power was lost to the entire building, and other floors still had commercial power. (Poor planning?) According to reports, a telephone company employee cut power to the whole building so as to get the emergency power to kick in, which it did, but fifteen minutes later the telephone switching system ran out of power. (Insufficient emergency power generating capacity?) Now the entire facility was out for another four and a half hours.

Follow-up, Mon, 19 Jul 1999 06:14:03 -0400

According to a report in the *Toronto Star*, Bell's repairs to its switching facility that failed in downtown Toronto could not be completed since the building is kept locked during the weekend. (Isn't security that prevents restoration of service not in fact security?) In what is said to be a separate incident, about 960,000 residents of a very nearby city found themselves cut off from 911 police emergency service. Some phones that tried to call the number were "frozen". After about 9 hours, Bell managed

to "call forward" 911 calls to the non-emergency police number, and three hours later full 911 service was restored. The cause of the failure is, apparently, unknown.

⚡ Computer startup circuits

"M. Simon" <mlsimon@mail.rkd.snds.com>

Fri, 16 Jul 1999 18:41:57 -0700

Starting up a computer system with all its necessary hardware in a known state is a notoriously difficult problem. There are so many opportunities for errors of omission. There are many and difficult interactions of hardware and software.

Because the circuits themselves are very simple the work is usually given to novices.

The real problem is that so few engineers are cross trained. Few hardware engineers know software and vice versa.

I blame this on unnecessarily complicated software compilers. Minimum competency in C takes six to twelve months. I can teach software competency in my favorite language in 4 to 8 hours. (I did it with some engineers in my mfg. plant about three weeks ago, so don't tell me I am smoking something)

If you are interested in the name of the language e-mail me. I am not interested in starting a general language flame war.

Simon

⚡ Netcom partial e-mail outage

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

Fri, 16 Jul 1999 08:50:48 -0500

For about 24 hours after 7pm on 14 Jul 1999, Netcom users with user names beginning with a, d, f, h, i, k, l, n, q, r, u, or v were unable to read stored e-mail, because of a hardware failure in a file server in Netcom's San Jose data center (now part of Mindspring). On 10 May 1999, an outage affected only users with names starting with the letter "d".

[Source: ZDNN

(<http://www.zdnet.com/zdnn/>), PGN-ed]

⚡ junkfilter vs. xxx.lanl.gov

Thomas Roessler <roessler@guug.de>

Mon, 19 Jul 1999 18:06:58 +0200

This is essentially a "for the record" contribution on a well-known risk:

False positives with content filtering.

Junkfilter (see <http://www.pobox.com/~gsutter/junkfilter/>) is a rather sophisticated set of procmail rules and regular expression lists designed to catch spam mail. I've been using it for a couple of months now, and it does a nice job in preventing at least some of that "make money fast" stuff from

coming through to me, while usually keeping false positives negligible.

Today, I started to obviously miss important messages on an internal mailing list. It turned out that junkfilter's body check module triggered on the string "http://xxx", as in "<http://xxx.lanl.gov/abs/quant-ph/9603004>". This URL was contained in one list member's new .signature.

The underlying problem is, in this case, drawing conclusions from a (partial) URL on the content referred to by this URL. (One may also criticize drawing conclusions from content referred to in e-mail messages to such messages qualifying as "spam". Anyway, it usually works. :-)

✶ "Bright Light" POP-based spam filtering: a bad idea

Lauren Weinstein <lauren@vortex.com>
Tue, 20 Jul 99 11:16 PDT

Greetings. Bright Light Technologies (<http://www.brightlight.com>), which sports an impressive list of technology partners and investors, has introduced a new "free" service to users of POP-based e-mail (previously Bright Light has apparently mainly worked through ISPs) that attempts to filter out most unsolicited e-mail (SPAM) before it reaches the user. They do this by trying to detect spam flowing around the net and then applying filtering rules. Rejected messages are pushed aside and can be viewed later

if the user wishes, and lists of rejected messages are made available.

I'm a long time spam-fighter myself--I maintain a public spam blocking list at <http://www.vortex.com>. I'm more than willing to declare the concept of trying to filter out spam (so long as there aren't too many false positives) to be a good one. Unfortunately, the method chosen by Bright Light for end-user POP use is a potentially major invasion of privacy--ironic in light of Bright Light's written statements that they want to "avoid the appearance of violating email privacy" (exact quote).

The problem doesn't take a masters degree in Internet engineering to understand. To use their new POP service, you have to route ALL of your inbound e-mail through Bright Light servers. Your POP account accesses Bright Light, then they login to your ISP to pick up your mail. It passes through Bright Light, and then to you.

From both a Privacy and Risks standpoint, it's hard to imagine a system more primed for potential trouble. Any centralization of e-mail handling systems in this manner, funneling in e-mail from numerous ISPs, represents an immense target for all manner of mischief--possibly even more attractive to problems than the largest individual ISPs. Systems failures and overloading can happen. Hackers can target the facilities. And of course, the concentration of e-mail traffic could make Bright Light the recipient of choice for legal actions, by those seeking to track or access e-mail

messages for any number of purposes (an increasingly popular legal maneuver, as you probably know). The requirement to provide such information could occur regardless of how little (or how much) of users' e-mail is "normally" stored on disk at the service (as opposed to passing through) in the course of routine operations. With this service, users now have two entities with which they have to entrust their e-mail--their "real" ISP, and Bright Light.

Bright Light has other products that send spam filtering rules directly to ISPs with the spam blocking applied at the ISP level--such services don't present these same concerns. The fundamental problem with the new service, aimed at individual POP e-mail users, is having the full text of users' total incoming e-mail passing through a centralized third party e-mail service outside of the users' direct control or affiliation.

This isn't rocket science--it should be obvious that this sort of centralization of actual e-mail traffic flow is exactly the *wrong* direction to be moving in. I'd recommend thinking long and hard before participating, as an end-user, in any third party service that asks you to route all of your incoming e-mail through them. Even with the best of intentions (and I assume these on the part of Bright Light), and even with a "free" service, the price is much too high.

My RealAudio "Vortex Daily Reality Report & Unreality Trivia Quiz" for 7/19/99 (see below for URL to the archive of segments) was devoted to this topic. Take care, all.

Lauren Weinstein <lauren@vortex.com>; Moderator, PRIVACY Forum
<<http://www.vortex.com>>; Member, ACM CCPP; Host, "Vortex Daily
Reality
Report & Unreality Trivia Quiz" <<http://www.vortex.com/reality>>

✶ E-mail attachments and local names

Avi Rubin <rubin@research.att.com>
Tue, 20 Jul 1999 17:46:58 GMT

I just had a mildly embarrassing incident because of a Netscape
mail
"feature" when sending attachments. I'm sure that other mailers
do this as
well. When attaching a file to an e-mail message, the local name
of the file
is included in the attachment. So, the recipient gets to see
the contents
of the file, as you would hope, but also the local name that you
gave
it. Imagine several possible embarrassing scenarios:

Attachment: our.most.gullable.client.invoice.doc
Attachment: proposal.with.doctored.data.xls
Etc.

It seems that the user should be able to rename the attachment
for the
purposes of the message or that the file should just be called
attachment1,
attachment2, ...

Avi Rubin

✶ Ab van Poortvliet: Risks, Disasters, and Management

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

Thu, 15 Jul 99 17:29:07 PDT

A really interesting book on risks in transportation:

Risks, Disasters, and Management:
Understanding the Management of High Risks and
Its Consequences for Passenger Safety
by Ab van Poortvliet

Eburon Publishers, P.O. Box 2867, Delft, The Netherlands, 1999

✶ REVIEW: "The Mythical Man-Month", Frederick P. Brooks Jr.

"Rob Slade, dotting grandpa of Ryan and Trevor" <rslade@sprint.ca>

Fri, 16 Jul 1999 08:33:03 -0800

BKMYMAMO.RVW 990502

"The Mythical Man-Month", Frederick P. Brooks Jr., 1995,
0-201-83595-9, U\$24.69

%A Frederick P. Brooks Jr.

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8

%D 1995

%G 0-201-83595-9

%I Addison-Wesley Publishing Co.

%O U\$24.69 416-447-5101 fax: 416-443-0948 bkexpress@aw.com

%P 308 p.

%T "The Mythical Man-Month: 20th Anniversary Edition"

Brooks' work on software management is a classic, but, even with a quarter million copies in print, it is more regarded than read. A great many can quote Brooks' Law ("Adding manpower to a late software project makes it later") without knowing that it was Brooks' who said it. Which is a pity.

I can fully agree with the promotional literature that says Brooks' work is "timeless." On the "influential" side, however, I have my doubts. If Brooks' truly had the influence he deserved, we would have fewer late projects.

Brooks was originally writing from his experiences as project manager for IBM's System/360, and later with OS/360. It is remarkable how well his ideas have stood the test of time. While today we would long for an operating system that was "bloated" to a mere 400K in size (and I still haven't figured out the "tables" that keep being referred to), the concepts outlined for project management are as sound today as when first set down. And the objections raised against sound management and documentation were as silly in 1975 as they are today.

Chapter one outlines the joy of programming, and any creative work, and how tragically that joy can be drowned in the crush of a badly managed project. Brooks shows very clearly how work can, and cannot, be partitioned in chapter two. A very interesting method of structuring a project team is given in chapter three, slightly weakened by the ship and surgical analogies which do not fully hold up in programming: software project teams are never faced with immediate life and death decisions. The problem of abstracting all "interesting" work to team leaders is examined in chapter four.

Chapter five notes a tendency to try to overcompensate for prior missed

opportunities, leading to software bloat. Team communication is looked at two ways in chapters six and seven. Project estimation, in chapter eight, is shown to be a poorly practiced art. Software bloat is revisited in chapter nine, and documentation in ten. Chapter eleven notes something we have lost sight of in our reliance on demo software: it isn't meant to be a mere GUI shell, but a working system that we make all the mistakes on. The need for tools, outlined in chapter twelve, is well accepted today, but the insistence on common tools would pull more than a few programmers up short. Modularity, promoted in chapter thirteen, is also praised today--but not always used. Chapter fourteen has a very solid grasp of the reasons for project slip. Documentation, of the right sort, is reviewed in chapter fifteen, including an attack on the venerable flowchart.

The preceding chapters are all essentially unchanged from the original 1975 edition. Chapter sixteen is Brooks' "No Silver Bullet" paper, wherein he opined (in 1986) that programming was an inherently complex and difficult task, and that no development in the next ten years would provide a productivity increase on the level of an order of magnitude. (It is interesting that Java was unleashed upon the world at the end of that ten year projection, but, three years later, it hasn't opened any programming floodgates either.) Brooks points out objections to "NSB" in chapter seventeen, and answers them. The first edition is recast in point form in chapter eighteen. Chapter nineteen analyses what was right and

enduring in
the initial material, and what was wrong in the first place.

An enduring classic that deserves to be read and re-read.

copyright Robert M. Slade, 1999 BKMYMAMO.RVW 990502
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

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



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 50

Tuesday 27 July 1999

Contents

- [One year in jail for not turning off cell phone](#)
[PGN](#)
- [Communications blackout in Morocco](#)
[David Mediavilla](#)
- [Phone outage in Plano](#)
[John P McGraw](#)
- [Double your treasure, double your fun...](#)
[Daniel P. B. Smith](#)
- [ActiveX Security concerns continue](#)
[Richard M. Smith](#)
- [DoD password management](#)
[Identity withheld by request](#)
- [Misplaced priorities with electronic hospital records](#)
[John Doyle](#)
- [Clinical disruptions following loss of telephone service](#)
[John Doyle](#)
- [Re: Anaesthetists' equipment](#)
[Daniel Paul Sheppard](#)
- [Re: Computer startup circuits](#)
[M. Simon](#)

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

One year in jail for not turning off cell phone

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

Thu, 22 Jul 1999 22:16:11 PDT

Neil Whitehouse has been convicted of ``recklessly and negligently endangering'' a Madrid-to-Manchester British Airways flight with 91 passengers. Despite multiple warnings, he refused to turn off his cell phone. He was sitting over the aircraft's fuel tanks in the wings.

<<http://www.zdnet.com/zdnn/stories/news/0,4586,2298512,00.html?chkpt=hpqs014>>

Communications blackout in Morocco

Mediavilla David <davidme.forum@bigfootNOSPAM.com>

Mon, 26 Jul 1999 16:35:28 +0200

According to the Spanish paper "El Pai's",
<http://www.elpais.es/p/d/temas/hassan/7has25b.htm> (in Spanish) :

Since Hassan II (king of Morocco) was entered in the Avicena hospital (in Rabat) until his death was officially confirmed, 4 hours passed. In that time, the Moroccan news agency MAP halted service, mobile phones stopped working and Internet connection was down.

David Mediavilla Ezquibela

⚡ Phone outage in Plano

"Mcgraw, John P" <john.mcgraw@eds.com>

Thu, 22 Jul 1999 08:57:07 -0500

The *Dallas Morning News* reports that 100,000 people in Plano, a Northern Suburb of Dallas, were without phone service for 9 hours when a battery failed in the switching office. I have been told that this office has two power sources coming from different grids, but it appears that they still have a single point of failure. The 911 service was out as well, and I was told that a house in my old neighborhood was badly damaged by a fire when the owner could not reach the Fire Department.
<<http://www.dallasmorningnews.com/metro/0721met1phones.htm>>

John P, McGraw, CISSP, Plano, TX 75024 1-972-605-6949

⚡ Double your treasure, double your fun...

"Daniel P. B. Smith" <dpbsmith@world.std.com>

Thu, 15 Jul 1999 21:02:42 -0400 (EDT)

"Treasury Direct" is the long-established U.S. Government service that enables individual consumers to buy U.S. Treasury securities directly from the government. Normally the securities are held in an account, and interest paid by direct deposit to your bank account.

A few weeks ago, I used the Treasury Direct Web site,

<http://www.publicdebt.treas.gov/sec/sectdes.htm>,

to purchase several thousand dollars worth of Treasury securities. It was very easy. A little too easy, it turns out.

First, Web access was automatically available to me, simply because I have a Treasury Direct account. I did not need to request or authorize it. This means that, in all likelihood, millions of people have Web access to their accounts and don't even know it.

Second, I only needed two pieces of identifying information for full access: my account number, and my Taxpayer Identification (Social Security) number. Conveniently, both of these are printed together on every one of my Treasury Direct statements.

Third, it appears as if no special authorization is needed to enable purchases--the same authorization that lets them deposit small amounts of interest to my account also allows them to withdraw large sums to cover my online purchases.

This all seemed a little flaky, but some part of my brain was convinced that since Amazon handles \$32.95 purchases perfectly, it MUST be OK to buy thousands of dollars worth of Treasury securities via the Web... and I wanted to buy the securities... and I didn't feel like hassling with phone calls and forms... so I went ahead and clicked the button.

I placed the order on 2 Jul, for delivery today, 15 Jul. I felt warm and secure because the screen display, which I immediately printed,

showed all
the correct information together with a confirmation number.

Tonight I found that exactly twice the amount I authorized has
been
deducted from my bank account, and exactly twice the amount I
meant to
purchase is recorded as being in my Treasury Direct account.

Now, Treasury securities are not a bad thing to have, and buying
twice as
many as I planned to is not the worst thing that could happen,
but, among
other things, this happens to leave the balance in my bank
account
slightly too low to cover an outstanding check I wrote to the
IRS...

Only time will tell whether this is a small problem that the
Treasury
folks will straighten out quickly and cheerfully... or whether
this is the
start of a vast bureaucratic Kafka nightmare that will leave me
an
embittered, enfeebled, quaking wreck. (HOW am I going to PROVE
that I
DIDN'T click the button twice? And that I DIDN'T get a SECOND
screen with
a second confirmation number?)

Meanwhile... the RISKS are obvious.

Daniel P. B. Smith <dpbsmith@world.std.com>

⚡ New ActiveX security problems in Windows 98 PCs

"Richard M. Smith" <smiths@tiac.net>

Thu, 22 Jul 1999 22:12:27 -0400

At work, I recently started using a new HP Pavilion computer

that is running

Windows 98. As part of ongoing research into Internet security issues, I

discovered that this computer was shipped with 2 ActiveX controls, which are

extremely dangerous. These controls can be easily misused on a Web page to

gain access to the computer and run programs. More worrisome however script

code can be embedded in an HTML Email messages and the controls accessed in

Outlook, Outlook Express, and Eudora. The controls are marked "safe" for

scripting even though they can do things like launch programs and read and

write the Windows registry.

Using these controls, some of the malicious things that can be done include:

- Automatically install a computer virus or other malicious software on a system.

- Turn off all Windows security checking, making a system wide-open for future attacks.

- Read personal files for the local hard disk and silently upload them to a remote Web site.

- Delete document files from the local hard drive.

- Remove Windows system files so that a system can no longer be booted.

With less than 30 minutes of effort, I was able to construct a test Email

message that downloads a Windows executable file from a remote FTP site and

installs it on the local hard drive using one of these ActiveX controls.

After the file is successful installed, it then is executed. For my test message, I download and run the Windows calculator. However, the Email message can download any Windows program such as the ExplorerZip virus or Back Orifice 2000 install program. In Outlook Express, this all happens automatically when the Email message is read. There are no attachments that have to be clicked on and no warnings with default security settings.

My test Email message contains only about 10 lines of JavaScript code to direct one of the HP ActiveX controls to do the download and run the program. Anyone with experience in JavaScript programming could easily duplicate the code that I wrote. For obvious reasons, I will not be publically releasing this test Email message.

Microsoft's Authenticode security system built into Internet Explorer is of no use here because the ActiveX controls are pre-installed on the computer and not downloaded from the Internet. Authenticode only allows users to prevent downloading of questionable ActiveX controls, not their execution once they are installed on a system.

The ActiveX controls are shipped on the HP system for use in system diagnostic package called SystemWizard. This package is a product of SystemSoft (<<http://www.systemsoft.com>>). The intention is these controls would only be used in SystemWizard and no where else. However, because the controls are marked safe for scripting, any Web page or Email message can

use the controls in any manner they like. The controls either never should have marked safe in the first place or the controls need to do their own security checking. Unfortunately neither precaution was taken.

The two SystemSoft controls are just thin wrappers around a number of Win32 system calls. The Launch ActiveX control allows a JavaScript program to run a DOS or Windows program and pass in command line parameters. The RegObj ActiveX control allows a JavaScript program to read, set, and scan registry keys. The controls are accessed on a Web page simply by including an HTML <OBJECT> tag with appropriate parameters. Pretty obviously, it is not a good idea to allow JavaScript programs to make direct Win32 system calls with such ease!

To give an idea how easy the Launch control is to misuse, the following JavaScript call will remove the contents of someone's entire "My documents" directory using the old DOS deltree command:

```
Launch('c:\\command.com', '/c deltree /y "c:\\My documents\\*.*"');
```

Both of the SystemWizard ActiveX controls were created last year and my understanding have been shipped on most HP desktop systems in the US retail channel for at least the last 6 months. The number of computers, which are vulnerable, is therefore quite substantial. The same controls may also be being shipped on other brands of computers.

After being alerted to the problems of these two controls, SystemSoft is

providing a patch file to fix the security holes. This patch file can be downloaded from their Web site at this URL:

<http://www.systemsoft.com/support/syswiz/index.htm>

In addition to the two SystemSoft ActiveX controls, I also found another ActiveX control pre-installed on the HP system with a privacy leak in it. The control can give out Windows 98 registration information such as name, address, and phone number to a Web site. This control was supplied by Encompass Corporation (now part of Yahoo) and is used in an ISP sign-up program. The control is marked safe for scripting on a new computer, but is marked unsafe for scripting the first time dial-up networking (DUN) is used on the system. This issue is specific to this machine/build of the software. Unfortunately on my HP system, I use a LAN connection to access the Internet and therefore the Encompass control stays marked safe for scripting forever and could give out registration information (limited to name, address, phone number) to a malicious person. Since I didn't use the dial-up portion of the ISP sign up, I just removed the registration application by going to the add/remove program files and choosing the "Easy Internet Access" application. The control also remains safe for scripting if one uses AOL as an ISP because AOL does not use DUN support in Windows 98.

Since Encompass has distributed versions of the software on a different machines, I've put together a demo page that will test a system

to see if the system has a version of the control that could release registration information to a malicious person. The test page can be found at:

<http://www.tiac.net/users/smiths/acctroj/reginfo.htm>

I also upgrade from version 4 of Internet Explorer to version 5 on the HP system. Unfortunately this upgrade installed yet another dangerous ActiveX control on the system. This control is the DHTML editing control, which can be easily misused to read files from the local hard drive and upload them to a Web server. This bug was discovered in March 1999 and has been fixed by Microsoft but the majority of IE5 users still are vulnerable because not many people know about the problem. A security bulletin and patch for this ActiveX control can be found on the Microsoft Web site:

<http://www.microsoft.com/security/bulletins/ms99-011.asp>

How did so many of these insecure ActiveX controls get installed on my computer in the first place? Because Internet Explorer (IE4 or IE5) comes bundled with Windows 98, it is becoming an increasingly popular for computer manufacturers to build specialized utilities for their PCs using IE4 just like HP has done. These utilities include registration software, ISP sign-up programs, and shells for running common applications. With Internet Explorer 4 it is very easy to develop user-interfaces for these types of utilities using standard HTML pages. ActiveX controls are then typically used in these applications to provide low-level access to the

Windows

operating system to do things like run applications, access the registry, or read and write files. These controls are only suppose to be used inside the applications they are designed for. However, IE4 has no built-in mechanism for restricting use of a particular ActiveX control to be used with particular Web pages. Therefore it is up to application developer to provide a security mechanism in their ActiveX controls.

After looking at the problems of the HP system, I decided to check out other new Windows 98 systems from other computer manufacturers for similar unsafe ActiveX controls. The first thing I discovered that is very common for manufacturers to ship utilities built as Web pages on their computers. Most of these applications included ActiveX controls for doing things like running programs and accessing the registry. The controls had names like "SpawnApp", "SafeLanuch", "RegRead", and "Run". However, because I didn't have direct access to these systems, I have no method to test to see if these controls can be misused or not. Because their is no built-in security system in place for pre-installed ActiveX controls it is up to the person who writes the control to make sure they are safe. I have inquired to a number of computer manufacturers about the controls I saw, but so far have not received back any responses. Given the subtle nature of ActiveX security issues, I wouldn't be surprised that other computer models have serious security problems also.

A typical Windows 98 system today ships with about 50 pre-installed ActiveX controls that are marked safe for scripting. Because ActiveX controls are Win32 programs it's not possible to really know if a control is really safe or not. The developer's claims about safety cannot necessarily be trusted. Without systematic and detailed testing it is not possible to know if given control is really safe. I don't believe full testing is really being done today. For example, here is information about another Microsoft ActiveX control that is still being distributed with the Windows 98 Resource Kit today:

<http://support.microsoft.com/support/kb/articles/Q218/6/19.ASP>>

This Resource Kit ActiveX control allows Windows programs to be executed from a Web page or HTML Email message.

What can users do about all of these different ActiveX security holes? One approach is download patches to fix security holes as they are found. Unfortunately for most user's it is not possible to know what ActiveX controls are even installed on their system, never mind knowing which ones are really safe. It might require going to 4 or 5 different Web sites just sees what security patches are available. A pretty impossible task for almost anyone.

One easy thing users can do is completely turn off ActiveX controls in Internet Explorer. This is done on the security tab of the "Internet Options..." command in Internet Explorer. This option however

is only available if the Web site that one goes to don't use ActiveX controls.

What can computer manufacturers and software companies do about the problem of security holes in pre-installed ActiveX controls? As it turns out, Internet Explorer 5 already offers a great solution. IE5 supports a new feature called HTML applications (or .HTA files). An HTML Application is built like a Web page but can only be loaded and execute from the hard drive. Because an .HTA file comes from the local drive and not the Internet, scripts on the page are a completely trusted and are allowed to use all ActiveX controls installed on a system whether the controls are marked safe or not. For an HTML application, none of its private ActiveX controls have to marked safe for scripting and therefore the controls cannot be misused on Web pages.

For current systems, my recommendation is that computer manufacturers need to review carefully all the ActiveX controls which are pre-installed on computers that are going out the door. In the review, each control needs to be checked for potential security problems. It is particularly important to look at controls, which make Win32 system calls to load and execute other programs, read and write files, and access the registry.

I've created a Web page on my personal Web site that will check to see what potentially unsafe ActiveX controls are installed on a system. The URL for the test page is:

<<http://www.tiac.net/users/smiths/acctroj/axcheck.htm>>

Security problems with ActiveX controls have been a concern for a long time, because these controls are binary programs that are allow to make any kind of Windows system call. The industry has mostly been worried about ActiveX controls that were intentionally created with malicious code. Microsoft addresses these concerns with the Authenticode security system which allows users to decide if they trust a particular author enough to run controls that the author has written. Authenticode is based on adding digital signatures to controls.

However, the pattern I see here is a much different issue. Instead we have computer and software vendors installing ActiveX controls on systems without any notification and these controls for whatever reasons contain security holes in them. As I've pointed out here, I found 4 different ActiveX controls on my HP system for 3 different vendors which compromised the safety on my system. Not exactly a great track record! Going forward I hope that PC makers take a closer look at that the ActiveX controls that they are shipping on their systems. You never know who might be using that hidden-away ActiveX to create problems for us computer users.

DoD password management

<[Identity withheld by request]>

Wed, 21 Jul 1999 22:29:29 -0400

[This message is from Department of the Army civilian who has had Military active duty (53) system administration duties. His or her identity is withheld for obvious reasons. PGN]

I am an employee (15 + years) in the Department of Defense. In the last few days I have received the most ludicrous requirement yet. It applies to every part of DoD. It requires us to change every password on every system and then power down and power up the system. I have been told this was signed off by the Secretary of Defense upon urging by his Joint Task Force for computer security. For Army systems, this came in the form of a majordomo message. Last night I found out that it the aftermath of an incident. Prior to this knowledge, a lot of us thought that this was just an exercise.

When the initial message came in, MACOMS (Major Army Command typically 4 stars), RCERTS, and other institutions were called to see if this was a hoax. It turns out it wasn't. They actually want us to complete this requirement in less than 4 weeks. Initially, we weren't told the reason for the requirement -- just to get it done.

Shortly thereafter, we received another report that tells us (1) not to use the word "password" when directing our users to do this, (2) to use verbiage to our users explaining the need for the password change that is untrue, (3) to have the users change their passwords themselves rather than

have the system force them to do it. On (2), I don't think they intentionally wanted us to lie; just obscure the reasons. I first take issue that they have us (Sys Admin/Net Admin) mislead our installation users (another risk). Along with every IT (govt. employee, contract, military) person whom I have talked to at my installation, I think this requirement is overkill. In addition to using a lot of resources, it causes us the question the credibility of the people who are making these decisions. This in itself is a major risk.

Other thoughts:

1. Some people and sysadmins have about (3-7) passwords for various systems. If they have to change all their passwords they are likely to recycle the same passwords, on different systems.
2. I have spoken with my counterparts at different Army installations. For the most part they want to define the problem away (i.e., NT domain account is not computer account -- it is a resource account).

DoD is starting to take computer security seriously. However, they are using sledgehammers to stamp out flies. By doing this they make us (sys admins/net admins) question their capabilities.

There are several issues here. (1) military Vs civilian, (2) overreliance on FUD contractors, and (3) honesty between levels of commands.

[Signed] A concerned but disillusion DoD employee

[There are certainly some pockets of enlightenment within DoD,

but there are also some incredible examples of ostrich mentality, with heads in the sand. By the way, changing passwords does not help if sniffers are already in place. The deeper problem, familiar to RISKS readers, is the pervasive use of fixed passwords in the first place. PGN]

⚡ Misplaced priorities with electronic hospital records

"John Doyle" <djdoyle@hotmail.com>

Thu, 22 Jul 1999 12:37:33 PDT

As most workers in healthcare computing know, the electronic hospital record is becoming increasingly important, as it offers a number of advantages over traditional paper records. Nevertheless, there are a number of conveniences associated with paper medical records, just as many individuals prefer to read a paperback book over reading from a video monitor. In my hospital, a large metropolitan teaching facility, patient demographic data (age, height, weight, allergies etc.) are collected at a computer workstation and stored electronically as well as printed out as part of the paper chart. Although I am very computer literate, in my routine hospital work I prefer to use the paper chart not only for its speed of access (our network can be frustratingly slow in times of peak load), but also because it is simply far more convenient to use at the patient bedside.

Whenever I write an order for a drug to be given, I naturally check the

patient printout to search for identified drug allergies. Unfortunately, it can sometimes be difficult to find the entry for allergies, since it is not highlighted in any way in the monotonous paper printout. Believing that easy recognition of allergies in the paper record would be in the best interest of the patient (as well as in the interest of the hospital, I might add) I called our hospital computer services department to suggest that allergies be noted in an easily recognized bold or italic font. After all, I knew from experience that the implementation of this was usually fairly trivial, merely involving some simple printer escape codes.

Their reply surprised me.

I was informed that this request would not be a priority, as their policy was that the electronic record was far more important than the paper record, regardless of my personal preferences. Thus, attention to improvements the paper record would happen only when the long list of planned improvements to the electronic record was completed. In fact, they pointed out that they saw the eventual elimination of the paper record as a good thing, regardless of what any physicians "in the trenches" might feel about any difficulties that might arise as a result. That was their decision, period.

Since improvements that would be expected to lead to a reduction in drug administration errors is an obvious good (at least in my eyes), the attitude and decision surprised me. Perhaps they might feel differently if a family member received an inappropriate drug by mistake.

D. John Doyle MD PhD FRCPC, University of Toronto and Toronto
General Hospital
djdoyle@home.com <http://doyle.ibme.utoronto.ca>

✶ Clinical disruptions following loss of telephone service

"John Doyle" <djdoyle@hotmail.com>

Thu, 22 Jul 1999 04:52:19 PDT

As noted in an earlier posting in this forum, the recent loss of telephone service in downtown Toronto disrupted life for many individuals. At my hospital the loss of outside telephone access, Internet access, paging services and Bell Canada cellular telephone service lead to special challenges. No electronic paging of physicians and other personnel was possible. Overhead voice paging helped in some cases, but this system does not work in our operating rooms! Because of the potentially life-threatening issues involved, a number of surgical cases were cancelled, including my second cardiac case. Regrettably, because of well-known backlogs in the Canadian healthcare system, some cancelled surgical cases may not be rescheduled for some time.

D. John Doyle MD PhD, Associate Professor, Toronto General Hospital /
University of Toronto djdoyle@home.com <http://doyle.ibme.utoronto.ca>

✶ Re: Anaesthetists' equipment (Doyle, [RISKS-20.49](#))

Daniel Paul Sheppard <dps@Cs.Nott.AC.UK>

Fri, 23 Jul 1999 16:19:50 +0100

I read with horror John Doyle's article in [20.49](#) about the patient monitoring systems regularly used in anaesthesia. The article seemed to suggest that a typical arrangement for such devices is that a number of sensors are connected to a single unit, under control of a single software system, to be displayed on a composite display. The problem being that when a system crashed (for whatever reason) the system needed to reboot, depriving the anaesthetist of sensory data during that reboot, and losing important calibration data.

Surely, a better design for such a system would be a number of quite separate autonomous units, perhaps with low resolution output, or even (in some cases) numerical displays or just flashing LEDs. These could be connected to a separate device which collated the information and displayed it in a convenient form on a high resolution display. If this display crashed, then calibration data stored in the sensor units would not be lost, and all the data would still be available (in a less convenient form, and without cross correlation, admittedly). If one of the sensor units crashed, then a trace would be lost on both the unit and the display, but other sensors would remain.

Perhaps the principal justification why units are not built in

this modular
way is one of cost.

✈ Re: Computer startup circuits ([RISKS-20.49](#))

"M. Simon" <mlsimon@mail.rkd.snds.com>

Thu, 22 Jul 1999 13:11:28 -0700

I am overwhelmed by the response.

My favorite language is FORTH.

Easy to learn.

Easy to write.

Easy to debug.

Well written (easy to teach) it reads like English.

Interactive.

Compiled.

Modern versions run as fast as compiled C.

Fed Ex uses it in all their portable package tracking terminals.

Sun uses it as the boot language of every Sun terminal (Stop A)

Your astronomy observatory probably uses it to run its
telescopes.

Hardware/Software design should be the way to go in embedded
systems. No

more separation of the disciplines. There is no way to
reasonably teach the

complications of C in addition to teaching hardware design. Not
enough

time. It would add at least a year to the curriculum.

Simpler easier to learn languages mean fewer errors.

Easier to test languages mean fewer errors.

The current favorite 'C' is not easy to write and not easy to
test.

And yes I have made a living writing C programs. A very good

living (I
really do love inefficient languages from a personal \$\$\$\$\$\$\$
perspective)

M. Simon

[GO(TO) FORTH and multiply? 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 20: Issue 51

Monday 2 August 1999

Contents

- [Critical Infrastructure Protection: Japanese toilets](#)
[Carl Landwehr](#)
- ["Heat wave"](#)
[Steve Summit](#)
- [Risks of on-line auctions: eBay scam](#)
[PGN](#)
- [Conversion service for viewable formats](#)
[Lindsay Marshall](#)
- [2nd-class invitation in Outlook](#)
[Thomas Gilg](#)
- [Re: Computer-based patient monitor problems](#)
[William Hutchens](#)
- [Re: One year in jail: Fear in the skies](#)
[Bob Frankston](#)
- [Re: ActiveX security](#)
[Peter da Silva](#)
[Adam Shostack](#)
- [Are you sure your host isn't being mail-blocked?](#)
[Thomas Roessler](#)
- [More on small problem escalates into major disruption](#)

[Doug Moore](#)

- [New version of an old scam](#)

[Mike Ellims](#)

- [Equivalence of logical and physical behavior...](#)

[James S Dukelow Jr](#)

- [Re: Cancelling errors, serendipity in avoiding risks, and Kepler](#)

[Jim Thompson](#)

[Felix Tilley](#)

- [Go FORTH and Multiply](#)

[Patrick E Kane](#)

- [Announcing Dependability.org](#)

[Chuck Weinstock](#)

- [REVIEW: "Internet Security with Windows NT", Mark Joseph Edwards](#)

[Rob Slade](#)

- [The Software Engineering Symposium '99](#)

[Carol Biesecker](#)

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

✂ Critical Infrastructure Protection: Japanese toilets

Carl Landwehr <carl.landwehr@mitretek.org>

Fri, 30 Jul 1999 08:48:32 -0400

NPR's Morning Edition had a brief story this morning on high-tech Japanese toilets that include functions such as auto seat raise, warm rinse, and hot-air blow dry. Some of these have recently been implicated as a source of fires in houses.

Reporter to woman shopping for toilet:

"Are you concerned about the possibility of fires?"

Woman (as translated):

"No toilet is 100% safe. I am willing to accept some risk."

Carl Landwehr, Mitretek Systems

[Does this give new meaning to "going down in flames"? It also links the "Royal Flush" brand name with a red-hot poker player. PGN]

⚡ "Heat wave"

Steve Summit <scs@eskimo.com>

Thu, 29 Jul 1999 07:24:22 -0700 (PDT)

I had a report (which I've been unable to confirm, despite the time I've spent waiting) that during the heat wave in the northeastern U. S. earlier in July, a "weather" command on some computer at MIT produced the following curious output:

```
athena% weather bos
Conditions at KBOS on 7/6/99 at 7:56 PM EDT (18:56 GMT)
  Weather: Partly Cloudy
    Temp: 2147483647 F (2147483647 C)
  Visibility: 10 mi
  Barometer: 29.72 inHg
    Wind: NE 13 mph
```

Needless to say, the particular temperature value shown is intriguing to the computer nerds among us! Steve Summit <scs@eskimo.com>

[Yup, it is 2**31 - 1. PGN]

⚡ Risks of on-line auctions: eBay scam

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

Wed, 28 Jul 99 10:28:25 PDT

eBay users have apparently been victimized by a nasty denial-of-service-like scam: Someone makes an early relatively low bid, then a totally out-of-line high bid (which discourages all other bidders), and then withdraws the high bid at the very last minute -- which is allowed by eBay. This is known as bid shielding. See a Website created by Jason Hamilton <http://mars.superlink.net/jason/ebay/> who was one of the victims.

Conversion service for viewable formats

<Lindsay.Marshall@newcastle.ac.uk>
Wed, 28 Jul 1999 09:57:41 +0100 (GMT)

<<http://TOM.cs.cmu.edu/intro.html>>

This site offers a service for converting different kinds of documents into "viewable formats". it not only does Web-accessible documents, but also files that it will import using the form protocol for files. Imagine the potential for stealing information that this service opens up!

<http://catless.ncl.ac.uk/Lindsay>

[But, security by obscurity does not work too well for strange formats.

PGN]

2nd-class invitation in Outlook

<Thomas_Gilg@ex.cv.hp.com>

Fri, 23 Jul 1999 15:32:18 -0700

One of our engineers has decided to leave and go back to school to complete her Ph.D. and enter teaching, a career move we all wish her the best in. Before a going-away party could be scheduled however, she ended up in an unusually contentious software design meeting with four other momentarily-combative engineers, including myself. It was ugly!

As I pondered whether or not I was out of line during the meeting, and how we could reconcile our differences so she could leave on a high note, our administrative assistant used Microsoft's Outlook/Exchange "meeting request" feature to schedule a lab-wide going away party. Unlike most engineers in the lab, I and one of the other combative engineers quickly hit the "accept" button which converts the e-mail based meeting request into a calendar item and sends a RSVP back to the meeting organizer.

A day later, an update was issued on the same meeting request, and I scanned the request for the change. While the lab-wide mail list alias "Lab.All" was still on the "Required Attendance" line, I and one other combative engineer were now explicitly listed, by name, on the "Optional Attendance" line. My heart sunk at the thought that some of us were no longer welcome at her going away party. Good friends for so long, how could one lousy meeting drive us apart?

After some tactful asking around though, it became clear that there were no hard feelings and no one had tagged anyone as optional. Ah, enter another

Microsoft Outlook/Exchange feature.

If a meeting request is sent to a mail list alias, and then individuals accept the request *and* use the option to e-mail back a yes/no response to the meeting organizer, Outlook/Exchange does not recognize that the individual(s) are part of the original mail list alias. If an update is then issued on the same meeting request, Outlook/Exchange treats the unrecognized names as optional attendees.

Depending on the issue at hand, being explicitly listed as "optional" can take on a whole lot of extra meaning. Who needs enemies when you have Outlook/Exchange ;-)

Thomas Gilg, R&D Software Engineer, Hewlett-Packard tomg@cv.hp.com

✶ Re: Computer-based patient monitor problems ([RISKS-20.49](#))

William Hutchens <wthutchens@spamlessmindspring.com>

Sat, 24 Jul 1999 01:53:38 GMT

As someone who plans to practice critical care medicine in the future, I read Dr. Doyle's posting in [RISKS-20.49](#) with interest. Although my clinical experience in considerably shorter (currently a senior Internal Medicine resident), I've noticed a number of incidents similar to that described by Dr. Doyle. Along the same lines, but more insidious, is the possibility of misinterpreting data because the computer processes the data in

a manner
different than one would expect.

Case in point: Among the data that ventilators give regarding a patient's status are two values related to how much air the patient is moving. One is the tidal volume (the amount of air moved in a single breath) and the other is the minute volume (the amount of air moved over the course of one minute). It's very easy to assume that the numbers being reported by the machine are the actual tidal volume (air moved in the last breath) and the actual minute volume (true amount of air moved over the preceding minute).

I've noticed that, at least on the ventilators used at my hospital, that this is not the case. Whenever we have an irregularly breathing patient, the reported minute volume changes very rapidly. Although I haven't been able to get a copy of the ventilator's manual to confirm my suspicions, it seems that the value reported as the minute volume is a calculated value based on the respiratory rate and the patient's last tidal volume.

The risk here is that someone might not realize this. In an irregularly breathing patient, a doctor, nurse, or respiratory therapist might take a quick peek at the minute volume, assuming that the value reflects that patient's status over the entire last minute (i.e. an average of an entire fast-slow cycle) instead of being a snapshot taken at a brief moment of time.

Also, in order to interpret the blood gases (a measurement of the pH, oxygen tension and carbon dioxide tension -- used to decide if any changes need to be made in the ventilator settings) of a vented patient properly, one should take into account the minute volume that the patient has at the time the sample is drawn. Our laboratory computer allows the resp. therapist to enter the vent settings and minute volume along with the blood gas result so that they appear in the lab report. The person drawing the blood sample has to report something to the lab regarding the minute volume and this is usually whatever he sees on the readout at the time he draws the gas. The risk here is that someone reviewing the medical record might see the spurious minute volume value and conclude that the clinician made an erroneous decision regarding the blood gas values when, in fact, his actions were correct.

For the record, the ventilator in question is a Siemens Servo 900C. My hospital also used the more advanced Servo 300 model, and I've noticed the same behavior in that model as well. (Anyone want to comment on the risks of designating a more advanced model with a lower model number?)(

⚡ Re: One year in jail: Fear in the skies (PGN, [RISKS-20.50](#))

"Bob Frankston" <BobRisks@Bobf.Frankston.com>
Thu, 22 Jul 1999 23:32:06 -0400

Re: (<http://www.zdnet.com/zdnn/stories/news/0,4586,2298512,00.html>)

The article on the jailing of a cell phone user in the UK continued with "The scientific evidence showed that there was a real possibility of risk," Ensor said". Of course, no references were given in the story. But they aren't necessary because we know that cell phones are immoral and dangerous and cause cancer. It reminds me of the moralistic attitude that made it so difficult to prove that ulcers were caused by bacteria rather than being punishment for a stressful (immoral) lifestyle.

The real risk of this nonsense is in relieving the airlines for responsibility for safety. Many people will not turn off their cell phones because they are too mundane to think about. Why no outrage at the airlines for such incompetent design? Of course, the real problem with cell phones is that they confuse the systems on the ground and planes already survive the lightening and other sources of radio noise.

But what does one expect from a system that provides only punishment for those who liberalize the rules? And where the issue is the perception of safety more than the reality.

[We received lots of e-mail on this topic, most of it suggesting that there is still little hard evidence of bad effects. PGN]

🔥 Re: ActiveX security (Smith, [RISKS-20.50](#))

Peter da Silva <peter@abbnm.com>

27 Jul 1999 22:55:29 GMT

I have long argued that the real problem with ActiveX is the inevitable proliferation of controls with security holes. Once an insecure applet is distributed, it can never be revoked because the signature is built into the applet... if you hit a site and it asks you to run an applet provided by Microsoft, are you going to say "no"?

Richard Smith's article indicates that the problem is much worse than I expected, and worse than he realises: patches to the applets won't help... malicious users can simply provide the old insecure versions on their websites as trojan horses, depending on social engineering to convince "enough" users to just blithely execute the apps.

No, any code that's automatically downloaded from the net (and that includes Office documents!) should be run inside a sandbox. For active content, there's Java. For Word, there's Word Viewer. For vendors who ship documentation as self-extracting archives and Excel spreadsheets, well, the best solution is education.

I'm glad that Microsoft has recognised this problem and is providing "HTA" pages as an alternative to marking applets as trusted. Let them save face, so long as the problem's fixed, and turn off ActiveX for all other purposes.

Peter da Silva <peter@baileynm.com>

⚡ Re: ActiveX security (Smith, [RISKS-20.50](#))

Adam Shostack <adam@netect.com>

Wed, 28 Jul 1999 14:50:21 -0400

Wasn't this the problem with Eudora executing Javascript in e-mail? It was (cached) on the hard drive, and thus safe? The core problem is that Microsoft is blurring the boundaries between the computer and the web. The problems that such blurring creates are subtle, often misunderstood, and hard to fix. Richard's proposed solution of HTA applications means that an attackers needs to get something to cache a file on disk, and something else to read it.

Or, "Beware of SystemWizards, for they are subtle..."

⚡ Are you sure your host isn't being mail-blocked?

Thomas Roessler <roessler@guug.de>

Thu, 22 Jul 1999 20:14:32 +0200

Are you operating a mail server at a university department, with lots of one-user machines, Unix and whatever, hanging around on your network? Is your host being used as a smart host by those end-user machines? You should better go to www.imrssi.org and check whether your mail relay is listed as an open relay there. The probability is high - but I'm sure you haven't been told that your machine is on the list.

IMRSS is scanning the Internet for open mail relays. They try to send a test message through your machine, and look whether it gets back to them. If that's the case, the IP address from which the message was delivered to them is considered to be an output funnel of an open relay, and added to their database of possible spam mail sources.

That database is available via DNS, ready to be used by any modern mail server software for blocking any mail which gets delivered from the IP address in question.

The problem: IMRSS is not going to tell you. But they are going to tell anyone who happens to ask them about your machine.

Obviously, this is bad style (as is the fact that you don't get reasonable contact information from their web pages, as is the e-mail autoresponse you get when you try to contact them, and so on).

There are some actual RISKS connected with IMRSS' approach, too.

For instance, you may learn about your outgoing server being listed with them from your users, whose messages get suddenly bounced from certain sites. Not grave, but not the thing you really want.

But worse: IMRSS is actually doing spammers a favor. Wanna spam through open mail relays? Just look out for your favorite university (or internet provider), and feed the IP addresses used by it to IMRSS. You'll get a nice list of open relay candidates, including the workstation in that professor emeritus' office the administrator doesn't really care about.

Possibly, you,
the spammer, know about this before the administrator has
learned that he
may have a problem.

I checked this for a major German university, and got several
dozen relay
output funnels, some of them corresponding to another dozen
input funnels.
The administrators have been notified.

Finally, suppose you use IMRSS' database to block e-mail. Be
assured,
they'll have lots of major relays listed there, possibly without
these
relays' administrators knowing about this. Are you really sure
that none of
your users or customers is expecting important or critical
messages from a
machine IMRSS considers to be a possible spam source? You
better be.
Because this is your RISK.

Web references:

- The initial announcement of IMRSS to the spamtools list:
<http://www.iecc.com/cgi-bin/artget?t19981208011>
- IMRSS' home page:
<http://www.imrss.org/>

✶ Further follow up - small problem escalates into major disruption

<dougmoore@ibm.net>

Wed, 21 Jul 1999 22:02:45 -0400

In the case of the phone lines that locked up when they could
not reach the

emergency 911 number --- when a major 911 system went down near Toronto (see previous message): That the phones lock up is an intentional feature so that the 911 operator has a chance to get the information about the calling number and send help even if the caller is unable to communicate. Unfortunately, the "lock up" does not time out even if the 911 system doesn't answer within any reasonable period, and so the phone can't be used to reach any other number. At least 24 people's phones are known to have locked up. Based on estimates from Peel police, there might have been another 110 or so calls that did not get through to 911. About half of calls to 911 in the area are typically genuine emergencies.

Meanwhile more four days later, Bell has still not restored full service to the downtown Toronto financial district after a disruption at a switching centre. (See previous message.) At least two Toronto Stock Exchange systems are still down, as are a number banking machines.

⚡ New version of an old scam

Mike Ellims <mike.ellims@pitechnology.com>
Mon, 26 Jul 1999 15:08:47 +0100

Mail is doing the rounds in the UK about an Y2K banking scam which goes something like this:

Someone calls telling you that they represented your bank, and that they were having difficulty meeting requirements to be computer ready for Year

2000. They say that all bank customers would need to transfer their accounts to a bond account, specially designed to protect their money until the bank can fully comply with the Year 2000 requirements. To verify they talking to the proper account holder, you need to confirm some personal information, i.e. account number, sort code, and verbal authorisation to transfer funds to into the specially designed account...

You can guess the rest.

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

⚡ Equivalence of logical and physical behavior... (Pereira, [RISKS-20.48](#))

"Dukelow, James S Jr" <jim.dukelow@pnl.gov>
Mon, 26 Jul 1999 11:59:23 -0700

> ... is current education in digital circuit design sufficiently attuned to
> the subtleties of the physical world, or do students have an overly
> simplistic view of how bits are represented in hardware? ...

I believe that people who design chips and other circuitry to perform specific logical computations are generally aware of the need to assess whether the physical behavior of their circuits actually implements the logical specifications. That is one of the basic uses of the public domain circuit analysis program SPICE and its variants.

That said, the complexity of large chips and the fact that their scale may be bumping up (down?) against quantum phenomena calls into question whether the equivalence of their physical behavior and logical specs can truly be verified.

Pereira is certainly correct about the deterioration of "continuous" math education.

Jim Dukelow, Pacific Northwest National Laboratory, Richland, WA 99352
jim.dukelow@pnl.gov [Standard RISKS disclaimers apply.]

✉ Re: Cancelling errors, serendipity in avoiding risks, and Kepler

Jim Thompson <jim.thompson@pobox.com>
Sat, 17 Jul 1999 15:17:15 GMT

In reading Henry Baker's thoughtful article, I am strongly reminded of something the late Isaac Asimov once said:

The most exciting phrase to hear in science, the one that heralds new discoveries, is not "Eureka!" (I found it!) but "That's funny..."

Asimov's point is similar to Baker's: that discovery is more driven by the desire to understand mistakes, discrepancies, and other "funnies" than by pure intellectual will.

Jim Thompson <jim.thompson@pobox.com>

⚡ Re: Cancelling errors, serendipity in avoiding risks, and Kepler

Felix Tilley <ftilley@goodnet.com>

Fri, 16 Jul 1999 19:55:49 -0700

A VERY excellent account of Kepler's achievements can be found in Arthur Koestler's book, the Sleepwalkers. As I remember, it was published in circa 1959. It should be in your local library. I encourage all to read it. It is a history of cosmology from the time of the ancient Greeks to Kepler and Newton.

As a side issue, the Greek who invented the Ptolomeian model of the universe also wrote a treatise on conic sections!!!! This is covered in The Sleepwalkers. I can't remember his name exactly - it may have been Apollonarius of somewhere (Perga??).

Felix Tilley in Tucson, Arizona

[ADDENDUM: Stasinios Konstantopoulos <konstant@let.rug.nl> sent us this:

Apollonios of Pergamos did indeed write 'Conic Sections' in the 3rd

century. But it is Ptolemeus of Alexandria who should be attributed

with the atavism of the Ptolemaikon (Ptolemaic? Ptolemeian?) system,

one century before that. PGN]

⚡ Go FORTH and Multiply

Patrick E Kane <kane@urbana.css.mot.com>

Tue, 27 Jul 1999 20:52:37 -0500 (CDT)

You mean:

* Forth Go

✶ Announcing Dependability.org

Chuck Weinstock <weinstock@sei.cmu.edu>

Wed, 28 Jul 1999 11:33:19 -0400

Dependability.org has been established by the IEEE CS Technical Committee on Fault Tolerance and IFIP Working Group 10.4 on Dependable Computing and Fault Tolerance to be a central source on the Web for information about dependable systems technology. We hope that you'll visit the site often.

In addition, the IEEE CS Technical Committee has established a mailing list for distribution of its newsletter. The newsletter is sent out on an irregular schedule and lists upcoming events and other news of interest to the dependable systems community. If you would like to subscribe, an easy to use subscription form is available at <http://www.dependability.org/> or you can send a message to <mailto:majordomo@dependability.org> with a body that says: `subscribe fttc <your-e-mail-address>`

We welcome additional sponsors. If your organization is interested in sponsorship please contact <mailto:weinstock@dependability.org>

⚡ REVIEW: "Internet Security with Windows NT", Mark Joseph Edwards

Rob Slade <rslade@sprint.ca>

Wed, 28 Jul 1999 09:50:15 -0800

BKINSCNT.RVW 990625

"Internet Security with Windows NT", Mark Joseph Edwards, 1998,
1-882419-62-6, U\$49.95

%A Mark Joseph Edwards mark@ntshop.net mark@ntsecurity.net

%C 221 E. 29th St., Loveland, CO 80538

%D 1998

%G 1-882419-62-6

%I Duke Communications/29th Street Press

%O U\$49.95 800-621-1544 970-663-4700 fax: 970-667-2321

%O www.29thstreetpress.com ccarmel@29thstreetpress.com

%P 515 + CD-ROM

%T "Internet Security with Windows NT"

The introduction states that the book is intended for those with little or no NT security knowledge, but I suspect that making this the sole resource for a new system manager would be a dangerous thing, since it provides the proverbial "little knowledge."

Chapter one gives the user or administrator too much and, at the same time, not enough background on TCP/IP. There is a lot of trivia that does not relate to security, while there is no discussion of, for example, dynamic re-routing, which would be important in future examinations of IP spoofing. The grab bag of mostly intrusion related information in chapter two is not terribly helpful in preparing a defence. It is not clear to me why this part is entitled "TCP/IP Essentials."

Part two outlines the basics of the Microsoft Windows security

model. There is little presentation of a conceptual understanding or framework of the foundation chapter three, which instead lists a number of terms and programs. The "how to" of simple security operations is more comprehensible in chapter four.

Part three talks about principles of network security. Chapter five does not deal with multiprotocol networks, but again lists an assortment of security concerns. A number of security threats are described in chapter six, but not in an organized fashion. (The virus information, obtained from the Semantec [sic] Anti-virus Research Center, is basically useless.) A number of aspects that should be addressed in a security policy are listed in chapter seven. Chapter eight discusses a number of client programs for NT, but without much security relevance. A number of attacks are tersely described in chapter nine.

Part four looks at firewalls. Chapter ten does a reasonable job of explaining the different types of firewalls, although it also includes some unrelated material. Some considerations for evaluation are given in chapter eleven.

Part five outlines the Microsoft Proxy Server. Chapter twelve runs through dialogue boxes in the Internet Information Server. The proxy server itself is described in chapter thirteen. Design issues are discussed in chapter fourteen. Implementation is talked about in chapter fifteen, although there

are a number of areas not completely covered. Some client considerations are mentioned in chapter sixteen. Seventeen looks at troubleshooting and maintenance.

The book can provide some useful material, although most of the utility comes from the appendices, listing quick suggestions and resource contacts, rather than the text itself. Much of the content is unfocussed and almost disorganized. Some topics included are not immediately relevant to security work, while other areas stop short of actually helping the user or administrator.

copyright Robert M. Slade, 1999 BKINSCNT.RVW 990625
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

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

⚡ The Software Engineering Symposium '99

Carol Biesecker <cb@SEI.CMU.EDU>

24 Jul 1999 21:20:47 GMT

The Software Engineering Symposium '99

August 30-September 2, 1999

David L. Lawrence Convention Center

Pittsburgh, Pennsylvania

Theme: Improving the State of Software Engineering:
Principles, Practices, and Projections

The SEI Software Engineering Symposium provides a forum for discussing currently applicable practices that software practitioners can

use today.

The 1999 Conference on Software Technology and Engineering Practice (STEP '99) will be held jointly with the SEI Symposium.

The STEP '99 conference is sponsored by the International Workshop on Computer-Aided Software Engineering, Inc. (IWCASE), an international association of users, researchers, and developers of software tools, methods, and technology, and by the IEEE Computer Society.

The Preliminary Program, including Exposition Information, Registration Information and forms, and Presenter Guidelines, is available on the SEI Web site at <http://www.sei.cmu.edu/products/events/symp>

Contact:

Symposium '99 Conference Coordinator
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
Phone: 412 / 268-3007
FAX: 412 / 268-5556
E-mail: symposium@sei.cmu.edu



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 52

Thursday 5 August 1999

Contents

- [Can You Trust AT&T Wireless PCS Text Messaging?](#)
[Lauren Weinstein](#)
- [EverQuest devours players' lives](#)
[Mich Kabay](#)
- [Microsoft Word footnote problems irks federal appeals court](#)
[Declan McCullagh](#)
- [Perceived medical risk must often substitute for actual risk](#)
[John Doyle](#)
- [Open-source anesthesia software article in Salon](#)
[Martin Minow](#)
- [Re: IMRSS and Open Mail Relay Scanning](#)
[Lauren Weinstein](#)
- [Re: Japanese toilets](#)
[Chiaki Ishikawa](#)
[Brian Randell](#)
[Colin Sutton](#)
- [Risks of RISKS](#)
[Brian T. Schellenberger](#)
- [eBay's response to the eBay scam](#)
[Ray Randolph](#)

● [Re: Go FORTH and Multiply](#)

[Leo Wong](#)

● [Re: Heat wave](#)

[David Wittenberg](#)

● [Info on RISKS \(comp.risks\)](#)

✈ **Can You Trust AT&T Wireless PCS Text Messaging?**

Lauren Weinstein <lauren@vortex.com>

Wed, 04 Aug 99 19:47:17 PDT

Greetings. Can you trust that messages sent via AT&T Wireless PCS Text Messaging will always be reliably processed and received? Unfortunately, the answer appears to be no. What's worse, when failures do occur, there may be absolutely no indication to the sender of the message that their communication has vanished into the ether. An an example of a serious risk associated with a more general class of modern, widely-used communications systems, I believe that this is worthy of a detailed explanation and significant concern.

The use of text paging directly to digital/PCS cellular phones is rapidly replacing the use of conventional numeric and text pagers. Such phone-based text messaging, actually called "SMS" (Short Messaging Service) has a number of advantages over older paging systems. One of its biggest benefits is that the network will normally store messages for some extended period of time (e.g. 72 hours) for delivery to the phone, if the target phone is off or out of range. When the phone again is available, the message

is delivered, and the network receives confirmation that the message was successfully delivered to the phone. SMS messages typically can range between 110 and 150 characters or so, depending on how they are submitted and various formatting considerations.

The usefulness of SMS has caused an explosion in its use for all manner of free and pay information and warning systems, where automated systems will send messages (usually via an Internet e-mail interface provided by the wireless carriers) to users. Such messages could be anything from critical status messages for system support or medical personnel, to news bulletins and stock price warnings to traders.

But how useful is the entire environment if you cannot depend on messages ever actually being delivered, and if messages can vanish into a "black hole" without any warning?

AT&T Wireless (ATTWS) has, as you might expect, one of the most extensive SMS implementations. They provide three interfaces to the service:

- * a web-based "form" interface: type in your message and hit send
- * a direct dialup interface for specialized text paging software's use
- * an Internet e-mail interface: messages are sent to <cellular-number>@<a specific AT&T site>

The Internet e-mail interface is by far the simplest method to use both for Internet-connected individuals and automated systems.

Unfortunately, it is also this interface that apparently has the most problems. Since phones are addressed via their mobile number without any additional access codes being required, anyone who knows a cellular number can "flood" a phone with messages, eating up a user's entire monthly message allocation in short order--there's no way for the phone user to control such access. There are also some "denial of service" issues associated with this same lack of access control.

But of even greater concern is the fact that text messages submitted to ATTWS via their e-mail interface, at least for delivery to phones in the Los Angeles area (I don't have info about other areas at this time--it might well be a nationwide issue) can frequently simply "vanish" after delivery to the ATTWS e-mail gateway. Such "vanished" messages are never delivered to the phone user, nor is any indication of a problem ever received by the original sender of the message.

When this problem was originally brought to my attention recently, I was initially a bit skeptical, but testing indicated that it is indeed the case. While messages submitted via the web or paging software dialup interfaces were reliably delivered to phones, it was not difficult to find instances of messages submitted to ATTWS via their Internet e-mail interface which had simply gone poof! Interestingly, these seemed to all occur in the weekend period (Friday night through Sunday morning), at least in my testing. In

all cases, Internet mail delivery logs showed conclusively that the messages in question had been accepted successfully by the ATTWS SMS e-mail server (which is actually labeled as an "airdata.com" server). But the messages were never delivered to the target phones.

My initial contacts with ATTWS customer service about this were not inspiring. While the front line folks tried to be helpful, they have very limited information to work with (this is unfortunately typical of ATTWS customer service in many respects--many seemingly simple questions may receive answers ranging from correct to totally wrong from different representatives).

In this case, one rep told me that they had "heard" that the web interface was better to use and more reliable, and that he'd heard about paging system problems on weekends. He suggested that perhaps they take the system down for testing on weekends. This of course, even if true, would not be an acceptable explanation for the permanent disappearance of potentially important text messages!

Eventually I found my way to an ATTWS manager, with whom I am in continuing contact. While he initially didn't seem to understand the issue--at one point asking me if I'd ever missed an old-style regular page and pointing out that ATTWS service doesn't cover all areas (neither of which are at all relevant to the store-and-forward SMS environment and the problems at hand), he did ultimately appreciate both the issue and concerns.

He promised to try track this down with the technical folks, and I am still hopeful of a response, but as of this time, I have yet to receive an explanation.

Since then, additional testing has revealed more vanished messages following the same pattern, including as recently as this past weekend. I've also received reports from other persons regarding related AT&T Wireless PCS text messaging problems using interfaces other than the Internet e-mail interface, but I've concentrated on the e-mail facet in this report since that's where my own testing revealed lost messages.

So, the moral of this story is actually pretty simple--it can be very risky to simply **assume** that messages sent through the ATTWS PCS Text Paging Internet e-mail gateway are actually being delivered to user phones, even if the messages are accepted by the ATTWS e-mail gateway itself. This should be kept in mind if you're expecting to receive important information or other messages via such a method. The end-to-end, store-and-forward sophistication of SMS should be able to avoid the whole concept of permanently "missed pages" in the conventional sense over reasonable periods of time. Unfortunately, it appears that with ATTWS, at least at present in some areas, this simply isn't the case.

I'll of course report back when more information about this matter is available.

Lauren Weinstein, Moderator, PRIVACY Forum, <http://www.vortex.>

[com](#); "Vortex

Daily Reality Report & Unreality Trivia Quiz" <http://www.vortex.com/reality>

⚡ EverQuest devours players' lives

Mich Kabay <mkabay@compuserve.com>

Fri, 30 Jul 1999 00:12:25 -0400

Hunter Godfrey is quoted as saying that EverQuest "is the digital version of crack." He has spent over 656 hours on the game in about four months, the equivalent of 82 8-hour days. There are over 150,000 players ``hunting monsters, collecting loot, and forging alliances in MUD world.' [Source: Noah Shachtman, EverQuest: the Latest Addiction, Wired Digital, 29 Jul 1999; PGN-ed]

[Watch out for network congestion on corporate systems when this infiltrates workplace networks. M.E. Kabay, PhD, CISSP / Director of Education R&D Group / ICSA Labs <<http://www.icsa.net>>]

⚡ Microsoft Word footnote problems irks federal appeals court

Declan McCullagh <declan@well.com>

Wed, 04 Aug 1999 14:40:40 -0700

The U.S. 7th Circuit Court of Appeals is peeved at Microsoft. Seems as though unlike WordPerfect, MS Word doesn't count properly

footnotes, and lawyers doing wordcounts have been running over length limits on briefs.

Naughty, naughty, say the judges, who kvetch: that MS "ought to make it

possible to obtain a count of words in footnotes attached to selected

text." The august three-judge panel has forwarded a copy of its design

recommendations to Redmond. More info in a Wired News story (4 Aug 1999):

<http://www.wired.com/news/news/politics/story/21096.html>

-Declan

⚡ Perceived medical risk must often substitute for actual risk

"John Doyle" <djdoyle@hotmail.com>

Sat, 31 Jul 1999 10:16:59 PDT

All human activities entail risk. Indeed, to live is to take risks.

In the medical realm, patients who undergo anesthesia and surgery are frequently concerned about the risks involved, such as the risk of *not waking up* (or as one patient put it, *waking up dead*).

The risk of death or brain damage to patients undergoing general anesthesia is remarkably low, particularly for healthy patients in modern hospitals.

When an accident does occur, its cause is often an error made by the anesthesiologist, either in triggering the accident sequence, or failing to take timely corrective action. The overall risk of death for general

anesthesia in all comers is in the range of 1 in 10,000, the exact estimate depending on how one separates anesthesia misadventures (such as airway problems) from surgical misadventures (such as accidentally avulsing an artery).

Risks for individuals with specific conditions are sometimes known, but usually not. For example, administering general anesthesia when a patient still has residual food in his stomach poses special risks since the food sometimes ends up in the lungs (known as aspiration), with consequences ranging from trivial to deadly. However, risk data specific to any patient in this situation are not yet available. For instance, factors such as the "state of the anesthesiologist", characterized in terms of alertness, vigilance, and competence, would also be important.

(Of course, anesthesiologists employ a few good tricks to reduce aspiration risk. One trick that is not generally used would be to suck out all the food under visual guidance using a gastroscope. However, this procedure in itself introduces new risks and is at best unpleasant in the awake patient.)

Some individuals are surprised to learn that in a great many situations (indeed, in most complicated clinical situations) the risks of anesthesia or surgery may not be even approximately known (as in known to within an order of magnitude). No algorithm yet exists that one can use to get quantitative risk estimates for all situations. An example illustrates the point.

Recently I was asked to give an anesthetic for a man with several serious heart problems, the most pressing being a chaotic heart rhythm known as atrial fibrillation, which the heart doctors planned to fix with a big electric shock to the chest under general anesthesia (cardioversion). Once atrial fibrillation has started, it must be fixed within 48 hours or it will be necessary to start anticoagulant therapy (administration of *blood thinners*) to reduce the risk of a stroke. We had about 30 hours left.

Because of concerns about harming the patient with a general anesthetic I initially recommended against the cardioversion (electric shock) procedure, viewing drug therapy to be a clearly safer alternative. The trouble with drug therapy, however, is that it is far less effective and in addition requires a much longer hospital stay. In other words, cardioversion was by far the quickest and more cost-effective choice, although drug therapy appeared to be the safer choice.

But the final twist that lead us to go for the cardioversion was that the cardiologist pointed out that if drug therapy turned out to ineffective in this individual by the end of the 48 hour window, the option of subsequent cardioversion could not again be exercised until 4 weeks of anticoagulant therapy had passed. The risks (such as the risk of bleeding) and costs associated with that option now made cardioversion seem more attractive.

The unique nature of this particular patient's problem list meant that any risk estimates from the literature would almost certainly be meaningless. It was therefore necessary to rely on judgement drawn from experience rather than formal risk data. Perceived risk must substitute for actual risk in many settings.

D. John Doyle MD PhD FRCPC, University of Toronto and Toronto General Hospital
djdoyle@home.com <http://doyle.ibme.utoronto.ca>

APPENDIX

The proposed drug therapy was intravenous amiodarone. Medical conditions included: recent myocardial infarct with impaired ventricular function, aortic stenosis, atrial fibrillation, gastroesophageal reflux (a *full stomach* equivalent situation.) The patient was also known to be very difficult to intubate because of a small chin! Finally, note that moderately reliable mortality estimates for multi-organ failure patients in Intensive Care Units can be obtained by using the APACHE II algorithm; this is one of the few situations where good risk data exist for complicated patients.

Open-source anesthesia software article in Salon

"Minow, Martin" <MMinow@itc-us.com>

Thu, 5 Aug 1999 07:57:03 -0700

Risks readers may be interested in an article by Andrew Leonard

in the
online magazine, Salon, on the risks (and potential advantages)
of
open-source medical software:

<http://www.salonmagazine.com/tech/feature/1999/08/05/anesthesia/index.html>

"When he isn't in the operating room taking care of patients, [Dr. Stefan] Harms is hacking on the five computers in his basement. And he thinks he knows how to achieve his dream of low-cost, reliable anesthesia software -- by going the open-source </tech/special/opensource/> route. Last year, Harms founded LAMDI, <<http://gasnet.med.yale.edu/lamdi/>> the Linux Anesthesia Modular Device Interface. Harms thinks that the open-source software development model, in which the source code to a program is made freely available to the general public for redistribution and modification, offers fruitful possibilities for addressing anesthesiological software needs. ...

"The obstacles faced by Harms in his quest for open-source anesthesia software suggest that there are some serious potential limits for the open-source software model. The experience of some medical programmers who have placed their code in the public domain indicates that open source is certainly no panacea for the problems faced by medical practitioners. But there are still some intriguing possibilities. If liability issues can be addressed, and if the peer-review component embedded in open-source software can be proven to result in pragmatically better software, then, suggest some

open-source enthusiasts, wouldn't it be our duty to proceed down the open-source road?"

(Transcribed by Martin Minow, minow@pobox.com, with apologies for any residual Windows formatting cleverness)

✦ **Re: IMRSS and Open Mail Relay Scanning (Roessler, [RISKS-20.51](#))**

Lauren Weinstein <lauren@vortex.com>

Mon, 2 Aug 99 19:16 PDT

In [RISKS-20.51](#), concerns were raised over <http://www.imrss.org>, their ongoing automated search for open mail relays, and the publicly accessible query database of the resulting data which they maintain. It was suggested that such a database might actually help spammers find potential relay targets.

I was also concerned about this, and sent them e-mail asking for clarification on a number of related issues. After several attempts (they have various automated responders I had to deal with) I was quickly rewarded with a phone call from Ron Guilmette, who runs IMRSS. We had a long and friendly chat.

While my own orientation towards fighting SPAM is different than his, and I do not agree with various aspects of his operation, I think it's worth noting that he seems quite level-headed and sincere, and clearly has a lot of experience in the real world of SPAM problems.

Also, they are apparently about to address one of the more serious criticisms of their procedures, by beginning a program to attempt to send notification messages to "postmaster" and/or related addresses (when these exist!) for sites where open relays are found. This will at least provide such sites with an early warning that they were found to have an open mail relay, and that they were added to the IMRSS database.

Lauren Weinstein, Moderator, PRIVACY Forum <http://www.vortex.com>
Member, ACM Committee on Computers and Public Policy

✶ Re: Japanese toilets (Landwehr, [RISKS-20.51](#))

Chiaki Ishikawa <Chiaki.Ishikawa@personal-media.co.jp>
Fri, 6 Aug 1999 01:33:43 +0900 (JST)

Well the joy and risk of high-tech toilet!

It must have been quite an amusing and hilarious way to really wake up to hear the interview on NPR (National Public Radio?). And many seem to think that the Japanese is too serious a nation without the proper sense of humour, but I digress.

The case, eh, the toilet in question was an 18 years old toilet that caused a minor fire in April this year (1999). The cause seems to be a trouble in electrical wiring due to leaking water.

Trying web search engines with "toilet fire" in Japanese didn't turn out

useful pages at all. Below is what I gleaned from an article at Mainichi Shimbun newspaper site (in Japanese).

By the way, fires believed to be caused by similar toilets were reported in October last year (1998), and July 1993.

The fire in April this year was believed to have happened in the following manner. The plastic vinyl water pipe (for supplying heated water, I think) degraded and water began seeping. The water caused the temperature sensor to get rusty. The rust caused the electrical resistance of some electrical contacts to go up much higher than it was supposed to be and thus the excessive heat was generated. Finally, the vinyl coating of the electrical wires caught fire.

The family members had noticed the little water seepage about half a year earlier, but did nothing since the basic functions of the toilet such as heater, etc. were still operational.

Many such toilets, of which life time the manufacturers say is about 7 years, are believed to be used in Japan. The fire fighting department of Tokyo government was quoted as saying that such toilets that outlived the warranty period ought to be checked early. (I could not find reference to the toilet at the fire-fighting dept. web site, though.)

In Japan, these type of toilets showed up in the market early 1980's. Today, about third of such toilets are this type according to a survey mentioned in the article.

Personally, it was shocking and amusing to find the toilets of this type when my office moved to a new building about 10 years ago. Being a gadget-interested person as I am, I tweaked the "control" myself. The reported toilets that have seat raise control must be the "Rolls Royce" of this type of toilets. The one at the office doesn't have such a luxury so to speak. Frankly speaking, I doubt if such toilets do exist: we need hydraulic piston or something for that, don't we? In a toilet?

Anyway, even the Mainichi article had to have a cute headline talking about this subject: it goes something like "Many fires by toilet: it smells and your bottom is on fire!"

Oh well. It was a good thing that the interview was not aired on April first. Nobody would have taken it seriously in USA.

Risks? We probably should not put electrical circuits unless absolutely necessary. Toilets are not thought of as the cause of fire at least by many. Of course, run-away faulty microprocessor or whatever will get you in a real trouble such as minor burn!

Ishikawa, Chiaki ishikawa@personal-media.co.jp.NoSpam
Personal Media Corp., Shinagawa, Tokyo, Japan 142-0051

✉ Re: Japanese toilets (Landwehr, [RISKS-20.51](#))

Brian Randell <Brian.Randell@newcastle.ac.uk>

Tue, 03 Aug 1999 11:13:04 +0100

> ... Some of these have recently been implicated as a source of fires ...

I was pleased to get the above explanation of at least some of the electronic controls on these toilets. Such controls are, not surprisingly a feature in the advanced research laboratory that I've visited regularly in Japan these last few years - one that I made a point of photographing for my unbelieving colleagues back here in the UK.

I had hinted to my hosts that I would appreciate English language instructions or even a manual, so as to understand the multiple buttons, keyboards, and digital displays (including of dates and times) - but neither were forthcoming. However, they did accept the possible validity of my concern that these toilets might well not be Y2K compatible - and we had some interesting speculations as to the likely forms and seriousness of the possible consequences! :-)

Brian Randell, Dept. of Computing Science, Univ. of Newcastle,
Newcastle
upon Tyne, NE1 7RU, UK Brian.Randell@newcastle.ac.uk +44 191
222 7923

✉ Re: Japanese toilets (Landwehr, [RISKS-20.51](#))

"Colin Sutton" <colin@sutton.wow.aust.com>
Tue, 3 Aug 1999 22:16:27 +1000

My wife and I went into a department store in Tokyo and she

visited the toilet. When she came out she was soaked and she couldn't stop laughing. After she'd used the toilet (and used it well) she went to flush it and discovered a row of pushbuttons with Kanji labels. Not wanting to leave the toilet in an unsuitable state for the next user, and not reading Kanji, she stood back as far as she could from the toilet and pressed one of the buttons. Hot air started to blow up from the bowl. She tried the next button, and got sprayed with water. Luckily it was winter and she was wearing a raincoat. The other buttons didn't seem to do much at all, perhaps adjust the temperature of the toilet seat or something. None of them caused the toilet to flush. So she gave up, turned to the washbowl (in the cubicle with the toilet, as they often are in Japan). When she turned the tap on, the toilet flushed.

A good design. And the Japanese are so fond of cute icons. It's a pity no one thought about the illiterate.

Colin Sutton, Development Manager, Siemens Building Technologies Pty. Ltd.

14-18 Suakin Street, Pymble NSW 2073 Australia +61 2 98551310

[What about the ill-litter-rate? PGN]

Risks of RISKS

"Brian T. Schellenberger" <bts@unx.sas.com>

Wed, 4 Aug 1999 10:57:03 -0400 (EDT)

A few miscellaneous risks from recent risks issues:

1. Risk of not explicitly stating the risk.

Marshall Lindsay wrote of the "Conversion service for viewable formats." Our Esteemed Moderator wrote: "But, security by obscurity does not work too well for strange formats."

This suggests to me that perhaps the risk that Mr. Lindsay was referring to wasn't sufficiently clear. The risk is not that formats are decoded; but rather, that the people supplying the conversion service could readily make a copy of every document passing through their translation service. Sooner or later they are likely to acquire plenty of interesting information!

2. Risk of promoting silver bullets.

M. Simon wrote a couple of articles; one teaser and one sort-of real article, promoting the FORTH programming language.

First of all, the "teaser" article should **never** have been printed in RISKS. It contained no actual information; it was just a shameless plug for something that wasn't even named.

Second, as I hope all RISKS readers know, there is no "silver bullet" to the programming challenges facing us, and this article certainly promotes FORTH as just that.

Third, I've used FORTH, and it is a lovely little language, but I think that it's a particularly poor candidate for such a silver bullet if one were to exist at all.

First of all, by its very nature it does not support static error

checking. It completely lacks the concept of a "type" which renders

its ability to do even run-time error checking very limited. It is

great for small projects and for controlling real-world objects.

(Controlling telescopes, for example; the application for which was

originally designed.) I cannot even begin to imagine managing a large

(hundreds of programmers) project with it, and I do not believe that

a project that takes hundreds of C or Java programmers could be done

with a mere dozen FORTH programmers, either. (Though a project that

takes a half-dozen C programmers may very well be doable by a single

FORTH programmer, and FORTH is underutilized, it's not a language

which scales up to enormous projects well, IMHO.)

3. Risk of waiting for risks to be proven.

Bob Frankston wrote of "Fear in the the skies" and stated that "The

real risk of this nonsense is in relieving the airlines for responsibility for safety" and Our Esteemed Moderator observed that

lots of e-mail had been received, "most of it suggesting that there

is still little hard evidence of bad effects."

All this is true, and yet when we weigh even slight evidence of risk

and the airlines responsibility for the safety of its passengers

against the rather minute convenience that a cellular phone offers on

a plane; and when we consider the social risks of allowing the passengers to determine which safety rules they will follow

and which

they will ignore when the well-being of their fellow passengers is at stake; I do not believe that the decision in this case was outrageous.

BRIAN TOD SCHELLENBERGER bts@unx.sas.com

✶ eBay's response to the eBay scam

"Randolph, Ray" <Ray_Randolph@kne.com>

Mon, 2 Aug 1999 12:47:25 -0600

The most astonishing part of the information provided in [RISKS-20.51](#)

regarding the eBay scam was the response from eBay found on the web site we

were pointed to (<http://mars.superlink.net/jason/ebay/>).

eBay's response,

"PLEASE, do not give out details of this, as it will only cause more users

to try it." Is classic security through obscurity. In this case, with all

of the media attention this is getting, certain eBay employees are no doubt

lamenting the Risks of the media discovering what they've attempted to

obscure. :)

✶ Re: Go FORTH and Multiply (Kane, [RISKS-20.51](#))

"Wong, Leo" <LRW@mail3.cs.state.ny.us>

Tue, 3 Aug 1999 08:54:00 -0400

> You mean:

> * Forth Go

One reason that Forth is simple is that it reads from left to right:

Go Forth AND *

Leo Wong hello@albany.net <http://www.albany.net/~hello/>

✉ Re: Heat wave ([RISKS-20.51](#))

David Wittenberg <dkw@cs.brandeis.edu>

Tue, 3 Aug 1999 08:57:13 -0400 (EDT)

> athena% weather bos
> Conditions at KBOS on 7/6/99 at 7:56 PM EDT (18:56 GMT)

Note also the unusual time conversion. 7:56 PM EDT is 19:56 EDT, which is 23:56 GMT, not the 18:56 they reported. Or is there an EDT

other than (American) Eastern Daylight Time, presumably somewhere in England?

--David Wittenberg

dkw@cs.brandeis.edu



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 53

Tuesday 10 August 1999

Contents

- [Cell Phones Become Instant Bugs!](#)
[Lauren Weinstein](#)
- [Cell phone sends jet off-course](#)
[David Clark](#)
- [Sharing files via Yahoo](#)
[Morten Welinder](#)
- [Executive Order on Unlawful Conduct on the Internet](#)
[Bill Clinton via PGN](#)
- [California's "shameful reputation"!](#)
[PGN](#)
- [NCIC 2000 Begins Operations](#)
[Jack N. Fenner](#)
- [Complexity and Safety in Medical Electronics](#)
[Dr D John Doyle](#)
- [Re: Go FORTH](#)
[M. Simon](#)
- [E-Trade and long passwords](#)
[Mark Harrison](#)
- [Security sites vandalized](#)
[NewsScan](#)

- [SPAM causes major ISP crash](#)
[Peter Leeson](#)
 - [Re: PCS, IMRSS, Mobile phones in airplanes](#)
[Peter Houppermans](#)
 - [Cell phones and aviation electronics](#)
[Glenn Carroll](#)
 - [REVIEW: "Kerberos: A Network Authentication System", Brian Tung](#)
[Rob Slade](#)
 - [UPCOMING EVENT- USENIX Security Symposium, 23-26 Aug 1999 in DC](#)
[Moun Chau](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Cell Phones Become Instant Bugs!

Lauren Weinstein <lauren@vortex.com>

Mon, 09 Aug 99 14:37:28 PDT

Greetings. A disturbing application for the new generations of digital cell phones appears to be developing -- many models can be easily used as remote-controlled clandestine listening devices ("bugs"), often with little or no modification.

It turns out that many current cell phone models can be set into modes where they are completely silent (no "boops" or "beeps") and will answer incoming calls automatically. This latter mode is designed for use in hands-free (headset) situations. A cell phone left in a strategic location set in such modes may be silently interrogated from virtually anywhere on the planet with a simple phone call, and will happily transmit the room conversations back to the caller. When the caller hangs up, the cell phone resets, ready

for the next call.

In some cases, phones can be placed into this "automatic answer" mode without any accessories being required. For some models, a headset connector needs to be plugged into the phone, which may be modified to allow the phone to continue using its built-in microphone when in its "bugging" mode, or could trivially have a remote microphone wired via a very thin cable to the actual cell phone some distance away.

Even without an outside source of power, many modern digital cell phones can have standby times of a week or more, and be able to transmit conversations for a number of hours. With an outside power source, they could perform their bugging functions indefinitely.

Since various commercial firms are now planning to offer a wide variety of location-based services using cell phone location tracking capabilities, (which were originally mandated for 911 use), it seems likely that planted cell phones may soon be usable to track the location of persons or moving vehicles as well. Just picture a cell phone hidden in a car trunk with a tiny microphone wired up behind the rear seat, for example. The car wiring would also provide an ideal source of continuing power for both bugging and tracking via the cell phone. Simple, cheap, and accessible from practically anywhere!

Cell phones can also of course act as communications platforms for a variety of other add-on devices, such as tiny cameras, small Global

Positioning

System (GPS) units (for highly accurate location tracking that works *today*), and so on. While the current generations of cell phones have fairly limited data rates, and there are a variety of technical analog vs. digital issues involved, many cell phones can still be used for such "enhanced" applications even in the existing limited data bandwidth environment. It must also be pointed out that a hidden cell phone could also be used to remotely control or trigger apparatus connected to the phone, under the command of the caller.

With cell phones becoming smaller and the associated networks ever more ubiquitous, this whole area has a great deal of potential for serious privacy-invasive and other abuses.

Lauren Weinstein

<lauren@vortex.com>

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

"Vortex Daily

Reality Report & Unreality Trivia Quiz" --- <http://www.vortex.com/reality>

[An earlier version of this appeared in Lauren's PRIVACY Forum Digest,

(<http://www.vortex.com/privacy/priv.08.11>)

Saturday, 7 August 1999 Volume 08 : Issue 11, which he has augmented for RISKS. PGN]

⚡ Cell phone sends jet off-course

"Clark, David" <Dave.Clark@BCHydro.bc.ca>

Mon, 9 Aug 1999 12:28:45 -0700

>From: "Telecom News - August 6-9, 1999" News Summary

> "CELL PHONE SENDS JET OFF-COURSE", *Ottawa Citizen*, 7 Aug 1999
>

> "A Chinese plane drifted 30 degrees off course because a
passenger failed

> to switch off his mobile telephone. A crash was narrowly
avoided after the

> cabin crew found the phone during a desperate search while
approaching

> Beijing airport. Mobile phones are banned on planes worldwide
but a direct

> link with instrument failure has never been proved. The
Beijing incident

> is likely to provoke new air safety fears in Asia where at
least one crash

> is attributed to on-board phone use."

Sharing files via Yahoo

Morten Welinder <terra@diku.dk>

Mon, 9 Aug 1999 21:02:59 +0200 (METDST)

I just met this ad on Yahoo:

Share all your important files with friends and co-workers
with Yahoo! Briefcase

I am tempted to upload a few years' worth of comp.risks archives.
Risks (familiar to faithful readers):

* Yahoo knows your secrets.

* Anyone who snoops their traffic knows them too.

* Anyone who asks Yahoo for your secrets knows them too. (Yahoo
has a bad reputation for just handing over stuff in order to

avoid trouble.)

- * When your boss finds out who knows his secrets, he probably will not remain your boss.
- * "Make telecommuting even easier!" Convenience for security.
- * "Access and share files, documents and photos from anywhere." Your files or anyone else's, that is.
- * "You'll be registered with all of Yahoo!'s services." Just in case you don't get enough e-mail as it is.

The only thing missing seems to be a small sign saying "Just kidding -- gotcha!".

Morten

⚡ Executive Order on Unlawful Conduct on the Internet

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

Mon, 09 Aug 99 20:50:48 PDT

THE WHITE HOUSE

Office of the Press Secretary
(Little Rock, Arkansas)

For Immediate Release
6, 1999

August

EXECUTIVE ORDER

- - - - -

WORKING GROUP ON UNLAWFUL CONDUCT ON THE INTERNET

By the authority vested in me as President by the
Constitution and the

laws of the United States of America, and in order to address unlawful conduct that involves the use of the Internet, it is hereby ordered as follows:

Section 1. Establishment and Purpose. (a) There is hereby established a working group to address unlawful conduct that involves the use of the Internet ("Working Group"). The purpose of the Working Group shall be to prepare a report and recommendations concerning:

(1) The extent to which existing Federal laws provide a sufficient basis for effective investigation and prosecution of unlawful conduct that involves the use of the Internet, such as the illegal sale of guns, explosives, controlled substances, and prescription drugs, as well as fraud and child pornography.

(2) The extent to which new technology tools, capabilities, or legal authorities may be required for effective investigation and prosecution of unlawful conduct that involves the use of the Internet; and

(3) The potential for new or existing tools and capabilities to educate and empower parents, teachers, and others to prevent or to minimize the risks from unlawful conduct that involves the use of the Internet.

(b) The Working Group shall undertake this review in the context of

current Administration Internet policy, which includes support for industry self-regulation where possible, technology-neutral laws and regulations, and an appreciation of the Internet as an important medium both domestically and internationally for commerce and free speech.

Sec. 2. Schedule. The Working Group shall complete its work to the greatest extent possible and present its report and recommendations to the President and Vice President within 120 days of the date of this order. Prior to such presentation, the report and recommendations shall be circulated through the Office of Management and Budget for review and comment by all appropriate Federal agencies.

Sec. 3. Membership.

(a) The Working Group shall be composed of the following members:

- (1) The Attorney General (who shall serve as Chair of the Working Group).
- (2) The Director of the Office of Management and Budget.
- (3) The Secretary of the Treasury.
- (4) The Secretary of Commerce.
- (5) The Secretary of Education.
- (6) The Director of the Federal Bureau of Investigation.
- (7) The Director of the Bureau of Alcohol, Tobacco and Firearms.

(8) The Administrator of the Drug Enforcement Administration.

(9) The Chair of the Federal Trade Commission.

(10) The Commissioner of the Food and Drug Administration; and

(11) Other Federal officials deemed appropriate by the Chair
of the Working Group.

(b) The co-chairs of the Interagency Working Group on Electronic Commerce shall serve as liaison to and attend meetings of the Working Group. Members of the Working Group may serve on the Working Group through designees.

WILLIAM J. CLINTON

THE WHITE HOUSE,
August 5, 1999.

<<http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1999/8/9/11.text.1>>

[For those of you whose systems lose the line overflow, that is <http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1999/8/9/11.text.1> concatenated with ?urn:pdi://oma.eop.gov.us/1999/8/9/11.text.1]

California's "shameful reputation"!

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

Sun, 8 Aug 99 13:32:01 PDT

In the **Sunday Examiner and Chronicle**, 8 Aug 1999, the **Chronicle's**

editorial ("Sunday" section, p.6) is titled "Silicon Valley Expertise Stops at Capitol Steps"; it begins with this statement:

In a cruel irony, the state that gave birth to Silicon Valley is also the state with one of the worst reputations for high-tech know-how at the government level. And it is a well-deserved, if shameful reputation.

This is prompted by the latest fiasco, the demise of

* A system supposedly linking county welfare offices (scrapped, \$18M lost)

The editorial notes the earlier failures familiar to long-time RISKS readers:

* Deadbeat parents' system (\$111M, abandoned) [[RISKS-19.12](#), [.43](#), [.73](#), [.82](#)]

* DMV upgrade (\$51M, abandoned) [[RISKS-15.80](#), [.82](#), [RISKS-16.01](#), [.07](#)]

* California Lottery agreement to improve Scratchers game (contract cancelled, \$52M lost after both sides sued) [not previously reported, although premonitions are noted in [RISKS-14.18](#) and [14.20](#)]

The editorial suggests that the new governor (Gray Davis) appears to recognize "that he has a critical role" to play, while asserting that the previous governor (Pete Wilson) "lacked sufficient interest".. The charge to improve matters rests with Elias Cortez, Davis' head of the Department of Information Technology (nicknamed ``DO IT''), who has put all new procurements on hold until Y2K is sorted out.

✦ NCIC 2000 Begins Operations

"Jack N." <jnf@pcisys.net>

Fri, 6 Aug 1999 14:21:32 -0700 (PDT)

The FBI has announced that the National Crime Information Center 2000 began operations on July 11. According to the FBI announcement (<http://www.fbi.gov/pressrm/pressrel/ncic2000.htm>), this is a major upgrade of the NCIC system which provides police officers nationwide with the ability to view mugshots, and perform fingerprint searches from their patrol vehicles. It also adds additional persons to the NCIC database, including persons on probation, on parole, in federal prison or with records as sexual offenders.

There are any number of risks associated with this system. Here are a few:

- 1) False positive matches on the fingerprint search. According to <http://www.civic.com/pubs/1998/september/civ-techsided1-9-14-98.html>, the NCIC 2000 fingerprint scan has an accuracy rate of 92 percent. (The original contract called for 100% accurate positive matches and 98% negative matches.) If false positives are a significant element of the 8% error rate, lots of people will be hauled to police stations and at least inconvenienced based on incorrect NCIC matches.
- 2) Lots more people in the database. The accuracy and timeliness of the information in this database must be questioned.

3) According to the same www.civic.com article noted above, no probable cause is needed for an officer to require a fingerprint image. In fact, the system is intended to be used to establish probable cause. If a match is indicated, the suspect is then to be taken in to a police station and the larger IAFIS fingerprint scan system used to confirm identification. (IAFIS automates the entire FBI fingerprint database, is not yet online, has an unknown accuracy rate, and takes 2 hours to perform searches.)

4) The NCIC 2000 project was twice as expensive (US\$183M vs US\$80M) and a took twice as long (7 years vs 3 years) as originally projected. Also, at least one of the original requirements (accuracy) was relaxed. Thus it shows the cost increases, schedule delay, and requirements fade often associated with large, ambitious projects.

5) One wonders how long it will be until this system will be used as a method of collecting and storing fingerprints on citizens not convicted--or even charged with--any crime.

Jack Fenner

✶ Complexity and Safety in Medical Electronics

"Dr D John Doyle" <djdoyle@home.com>

Thu, 5 Aug 1999 22:34:26 -0400

Some technologies, like scissors and chop sticks, are inherently simple.

Others, like nuclear reactors or life support electronics, are inherently complex. By nature, the safety issues associated with complex systems are more involved than those associated with simple systems. There are always added cost requirements in complexity, such as special requirements for ensuring the safe operation of the system. But the very subsystems added to increase safety necessarily add to complexity, and, ironically, enrich the number of possible failure modes in the overall system. Thus there is the concern that the failure of any add-on safety system may sometimes actually lead to new system failure modes that would not have otherwise occurred.

Consider the following hypothetical example:

A sensor failure or algorithm failure in a patient monitoring system results in a false "asystole" alarm in a patient monitored during general anesthesia. (This alarm indicates that the patient is in cardiac arrest, an obviously grave situation. However, every single unexpected asystole alarm I have witnessed to date has been false.) In a panic from seeing this unexpected alarm, an inexperienced physician taking care of the patient forgets to check for the absence of a pulse to confirm that there is indeed a problem. Instead, the doctor calls for the crash cart and immediately administers a full ampoule (1000 micrograms) of adrenaline to restart the heart.

Trouble is, the heart was doing just fine until then. There was no asystole, no cardiac arrest, just an algorithm failure that occurred from

a normal but low-amplitude electrocardiogram, possibly due to electrode misplacement.

Now the patient really is in trouble from a massive cardiac stimulant overdose!

Of course, this failure mode would not have occurred if no asystole monitor was used.

An interesting book which discusses these and other issues is: Robert Pool.

Beyond Engineering: How Society Shapes Technology. Oxford University Press.

New York. 1997. 358 p. \$30. (Reviewed in IEEE Spectrum May 1998).

D. John Doyle MD PhD FRCPC

University of Toronto and Toronto General Hospital

djdoyle@home.com

<http://doyle.ibm.utoronto.ca>

APPENDIX

While 1000 micrograms (mcg) is a good starting dose in a full cardiac arrest setting, in the normal intact heart it is a massive amount. Only a 10 mcg dose of adrenaline is needed to "rev up" a normal heart. With a 100 mcg the heart operates well beyond its safety region, at least in the elderly or the sedentary. With 1000 mcg doses of adrenaline most healthy hearts are at least moderately damaged, even when aggressive attempts at correction with other (also dangerous) drugs is attempted (as many published clinical reports of such drug error accidents will attest to).

⚡ Re: Go FORTH

"M. Simon" <mlsimon@mail.rkd.snds.com>

Fri, 06 Aug 1999 17:57:01 -0700

Elizabeth Rather might disagree with you about large FORTH projects

(President of FORTH Inc). FED-EX has 1500 programmers doing mostly

FORTH. They claim it is at least 6X to 10X as productive as C.

Let's suppose FORTH does not scale well with more than 10 programmers. If

you get a 10:1 productivity improvement you might handle projects up to 100

ordinary programmers/coder/testers. The product will be better designed and

likely better debugged.

Very few projects require more than 100 software people.

I have found that testing each module as it is designed (easy in FORTH)

eliminates the need for type checking. Generally the quality of the code is

better because of this as well.

A 10-fold improvement in software engineering productivity is nothing to

sneeze at.

PS. Every place I have been allowed to use FORTH, it has been a magic

bullet. Perhaps I am unique.

⚡ E-Trade and long passwords

"Mark Harrison" <markh@usai.asiainfo.com>

Sun, 8 Aug 1999 22:31:13 +0800

I recently filled in an account application at etrade.com. I selected a RISKS-aware password, submitted the form, and received the following error message:

>Please correct the following information:

>

> Your Password must be 6 characters or less.

Yikes!

Mark Harrison, AsiaInfo Computer Networks, Beijing, China /
Santa Clara, CA

markh@usai.asiainfo.com <http://usai.asiainfo.com:8080/>

Security sites vandalized

"NewsScan" <newsscan@newsscan.com>

Fri, 06 Aug 1999 07:41:58 -0700

Just days after the Symantec site was attacked, vandals intruded upon

AntiOnline, another Internet site devoted to computer security.

The intruder

never directly infiltrated AntiOnline's own computers, but managed to

redirect visitors to a Web page with the image of an unblinking eye and the

message ``expensive security systems do not protect from stupidity.''

AntiOnline's manager said the attack was "clever" but not "sophisticated."

One security expert said, "All you can do is try to keep ahead of the game.

For anybody to claim they're totally secure, it's not true." [Source:

AP/*San Jose Mercury News*, 6 Aug 1999,

<http://www.sjmercury.com/svtech/news/breaking/ap/docs/7276141.html>

[NewsScan Daily, 6 August 1999, with permission. NewsScan is underwritten

by Arthur Anderson and the IEEE Computer Society. To subscribe to NewsScan

Daily, send an e-mail message to NewsScan@NewsScan.com with 'subscribe' or 'unsubscribe' in the subject line.]

⚡ SPAM causes major ISP crash

"Peter Leeson" <Peter.Leeson@ispi.co.uk>

Fri, 6 Aug 1999 09:21:34 +0100

Globalnet, one of the main ISP in the UK had their e-mail severely handicapped by a massive SPAM mailing from a Florida-based ISP. Mail was delayed by up to a day while the spam was cleared on 5 Aug 1999, slowly and painfully...

Peter Leeson

⚡ Re: PCS, IMRSS, Mobile phones in airplanes ([RISKS-20.52](#))

Peter Houppermans <Peter.Houppermans@pa-consulting.com>

Fri, 6 Aug 1999 03:31:36 +0100

I'd like to comment on three articles in [RISKS-20.52](#):

1) Re: Can You Trust AT&T Wireless PCS Text Messaging?

There are generic issues of dependency with mobile phone services. I have experienced several times that messages left for me on voicemail (as I was on the phone at the time) did not trigger the alarms on the

voicebox to alert me until fully 8 hours later (causing the ones that were urgent to be mildly out of date). This was on UK Vodaphone, and it occurred with both the 'call-back' service -it rings you and plays back the message- and the SMS service (it leaves an SMS alert message). Queries to the operator didn't yield a satisfying result, but to be fair, they didn't give me an SLA on performance and timeliness, I was getting used to it being quite immediate prompting an assumption on my part.

Another issue with voiceboxes is that they generally do not offer a method to play back a message you've just left, so if the line is bad you won't know the message (and return number) is next to useless for the recipient.

The RISK: don't rely on external facilities if the message is urgent, keep trying.

Note: the SMS services, however, give good feedback on message receipt.

This could mean a small risk: someone can tell my phone has been switched on and is within range of the system ;-)

2) Re: IMRSS and Open Mail Relay Scanning

Question: if IMRSS enters a company mail server into their list as 'open' and other companies use this as 'spam relay block' source, what is the exposure RISK to IMRSS for creating in effect a partial denial-of-service?

To leave a corporate mail server open for abuse is of course not a terribly good idea, but entering a server in the list of doom without the

target
companies' knowledge could IMO have legal consequences. The
planned
postmaster notification (maybe a with some time in between) is
therefore a
good thing.

Leads to another question: how is the company going to
communicate with
IMRSS? I presume it won't be by e-mail unless IMRSS don't they
use their own
list ;-).

3) Re: risk of using mobile phones in airplanes.

I've read this morning in the Hong Kong Standard of a plane that
was found
30 degrees off course when they were about to land (I have to
claim lack of
knowledge here: wouldn't this show up earlier?). When
researching they
found a mobile had been inadvertently left on by a passenger who
was too
preoccupied with a family member being ill (the reason he was on
that
flight) to check that his phone was off. The passenger has been
charged,
which must adds nicely to his worries.

The RISK: dependency on passengers to check their electronic
gadgets/phones
to be switched off. I would much rather see some form of
detector being
developed, at least that would start a flight with all mobiles
off. It
would then only leave deliberate actions like the individual who
continued
to use his phone despite requests to switch it off.

Peter A B Houppermans, PA Consulting Group +44 (0)207 730 9000

✈ Cell phones and aviation electronics (re: Fear of Flying)

Glenn Carroll <gcarroll@lmi.net>

Sun, 8 Aug 1999 11:52:13 -0700 (PDT)

Both the original "Fear of Flying" post and the follow-up have glided over another RISK: the airlines have no effective way of controlling or checking the state of cell phones or other portable electronics. As a sometime cellular user, I often forget that I have the thing with me, and I do enough flying that I tend to doze through the safety announcements, including the one which reminds passengers to "please turn off all cell phones, portable electronics, etc". Thus it isn't hard for a well-intentioned but forgetful person to create this risk-y situation. Lacking the means to find active portable electronics, the airline can't do much about this, nor can they prevent quietly malicious persons from deliberately doing the same.

Even non-forgetful people can inadvertently and unknowingly have their portable electronics on: CD players generally have their buttons placed in such a way that squeezing the case the right way will turn them on. Mine has a "lock" slider to prevent this from happening, but of course that's one more thing has to remember, and not all CD players come so equipped.

If cell phones or other p.e.s were as dangerous as some people claim, one might have expected a terrorist attack via this channel by now. After all, this would solve one of the difficult problems for the

terrorist, which is
how to get the Harmful Device on board the aircraft. Either
there have been
no such attacks, or they have been so ineffective as to go
unnoticed...

✂ REVIEW: "Kerberos: A Network Authentication System", Brian Tung

Rob Slade <rslade@sprint.ca>
Mon, 9 Aug 1999 08:54:34 -0800

BKKRBROS.RVW 990715

"Kerberos: A Network Authentication System", Brian Tung, 1999,
0-201-37924-4, U\$19.95/C\$29.95
%A Brian Tung
%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8
%D 1999
%G 0-201-37924-4
%I Addison-Wesley Publishing Co.
%O U\$19.95/C\$29.95 416-447-5101 fax: 416-443-0948 bkexpress@aw.
com
%P 164 p.
%T "Kerberos: A Network Authentication System"

Part one is a user guide to the Kerberos security tool, user
being defined
as both end user and administrator. Chapter one presents a
rather weak
justification for Kerberos (based on the insecurity of e-mail)
and some
quick contact information for obtaining it. End user operations
for
Kerberos are described, but not always clearly, and some
questions are left
open. (Does the user have any control over ticket expiry
times?) The

administrative functions, in chapter three, are weak in regard to installation, but reasonable in terms of maintenance operations. Chapter four contains quick listings of the Kerberos API (Application Programming Interface) calls, for those who want to build Kerberized programs.

Part two provides some background. Chapter five is a good tutorial on the concepts: if you are having trouble with chapters two and three, a review of five will probably help a lot. Differences in versions of Kerberos are listed in chapter six. A look at various related issues in chapter seven includes a very decent discussion of public key encryption.

For quick coverage of Kerberos, this makes a neat and handy package.

copyright Robert M. Slade, 1999 BKKRBROS.RVW 990715
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

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

✶ UPCOMING EVENT- USENIX SECURITY SYMPOSIUM, 23-26 Aug 1999 in DC

Moun Chau <moun@usenix.ORG>
Tue, 10 Aug 1999 00:27:34 GMT

8TH USENIX SECURITY SYMPOSIUM
23-26 August 1999

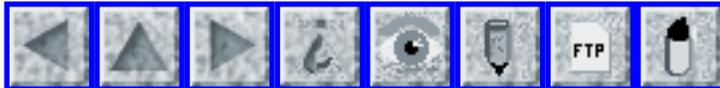
JW Marriott Hotel, Washington, D.C.

Sponsored by USENIX in Cooperation with the CERT Coordination Center

See the Program and register online at <http://www.usenix.org/events/sec99>

- * Exchange ideas with the industry's top security insiders.
- * Gain command of leading-edge tools and techniques at specifics-driven tutorials.
- * Explore the latest advances in Internet security, intrusion detection, distributed systems, and applications of cryptography.

USENIX, the Advanced Computing Systems Association, is the international, not-for-profit society made up of scientists, engineers, and system administrators working on the cutting edge of systems and software. For 25 years USENIX conferences and workshops have emphasized quality exchange of technical ideas unfettered by stodginess or commercialism.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 54

Sunday 15 August 1999

Contents

- [MCI WorldCom frame-relay network problems](#)
[PGN](#)
- ["Spy Who Messaged Me" -- now playing at Microsoft!](#)
[NewsScan](#)
- [High-flying hijinks: canine passenger sinks teeth into plane](#)
[Paul Costalas](#)
- [Risks of the modern train](#)
[Ben Hutchings](#)
- [Car won't start if payments are delinquent](#)
[Daniel P. B. Smith](#)
- [Salary payment diskettes intercepted and manipulated](#)
[Peter Fokker](#)
- [Risks of Internet Explorer 5](#)
[Lloyd Wood](#)
- [Refrigerator gasket frozen out](#)
[Ted Lee](#)
- [Y2K upgrade went 'horribly wrong', admits utility giant](#)
[Doneel Edelson](#)
- [Government: Lessening risks through encryption](#)
[Alan DeKok](#)

● [Having private services such as voicemail on shared phones](#)

[David Crooke](#)

● [Re: NCIC 2000](#)

[Stephen Fairfax](#)

● [Computers, Freedom, and Privacy: CFP for CFP](#)

[Bruce R Koball](#)

● [Info on RISKS \(comp.risks\)](#)

✶ **MCI WorldCom frame-relay network problems**

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

Sat, 13 Aug 1999 10:12:17 PDT

Almost one-third of MCI WorldCom's long-distance frame-relay network customers experienced difficulties, beginning on 5 Aug 1999, apparently as a result of a Lucent software and hardware during a network upgrade. (AT&T had a similar outage in April 1999.) The Chicago Board of Trade trading system failed, and problems there persisted into the following week. ATMs (teller machines) were rendered inoperative. [We await a more definitive analysis than could be gleaned from the various media reports.]

✶ **"Spy Who Messaged Me" -- now playing at Microsoft!**

"NewsScan" <newsscan@newsscan.com>

Fri, 13 Aug 1999 08:11:18 -0700

In the middle of the Microsoft-AOL battle over Microsoft's attempt to clone AOL's Instant Messaging system (which allows users to chat over the

Internet), an unidentified "overpassionate" Microsoft employee has embarrassed the company by getting caught in a little industrial espionage.

The rogue spy, whom Microsoft has acknowledged to be almost certainly one of its employees, falsely alleged in a message sent under a bogus identity that the AOL program contains an error responsible for creating a security

vulnerability. (*The New York Times*, 13 Aug 1999)

<http://www.nytimes.com/library/tech/99/08/biztech/articles/13soft.html>

[NewsScan Daily, 13 August 1999; reproduced with permission.

To subscribe or unsubscribe to NewsScan Daily, send an e-mail message to

NewsScan@NewsScan.com with 'subscribe' or 'unsubscribe' in subject line.]

⚡ High-flying hijinks: canine passenger sinks teeth into plane

<paul.costalas@telos.com>

Fri, 6 Aug 1999 17:33:03 -0400

Read the full story at the address below:

<http://www.phillynews.com/inquirer/99/Aug/06/national/DOG06.htm>

["Spread

the news" is a service of Philadelphia Online <http://www.phillynews.com>]

This is a very interesting story about how a dog in the cargo bay was able to free itself and almost bring down a 767. The dog had managed to "gnaw into wires" that affected the landing gear, flaps, and cockpit warning lights.

They are trying to figure out how the dog got out of its cage.

I wonder if anyone is focusing on why the wires were accessible to the animal. I am not an aviation expert, but could the wires be accidentally cut by a sharp edge, etc.? Why aren't the wires better protected?

Or is this the act of an angry animal striking out at the owners who neutered him?

Paul J. Costalas <paul.costalas@telos.com>

[Perhaps the dog was tired of listening to all that electrical energy flowing, and was a wire-heard terrier? PGN]

⚡ Risks of the modern train

Ben Hutchings <womble@zzumbouk.demon.co.uk>

Fri, 6 Aug 1999 23:11:08 +0100

I was quite impressed by the apparent quality of the new rolling stock of the Anglia train I caught from Ely last Friday evening.

This changed somewhat when I realised that although it was getting dark outside there were no lights on in my carriage. I turned on the back-light of my palm computer and continued to use it. Then, a few minutes later, I felt the need to use the lavatory. When I turned around to walk up the train, I saw that the next carriage was properly lit. In the lavatory there was no light - and no flush, no water and no hand-drier. This is because they all relied on electronic sensors. Furthermore, the doors to the next

carriage were also inoperative! Thankfully, the announcement system and the doors to the outside did work.

I moved up the train at the next station and found another lavatory. This one was designed for use by wheelchair users (as well as the able-bodied). The door is operated by yet more electronic switches - an open/close button and a lock button with a indicator. There are no instructions explaining what these do - just those labels. The open/close button works as I expected. By observation I deduced that the indicator is unlit when the door is open, flashing when it is closed but unlocked, and constantly lit when it is locked. The lock button takes the door from the closed state to the locked state or from the locked state to the open state. This behaviour does not seem very intuitive to me, and I have dealt with some fairly arcane interfaces! It was not until I left the lavatory that I understood that I had not successfully locked it.

I overheard two members of the train staff talking about the problems of the train. One described a potential denial-of-service in this toilet. It is apparently possible to put the door in the locked state by pressing the lock button while it is closing; this means that an attacker can press both buttons and leave before the door has completely closed. However, the door closes shortly after an occupant leaves, and this leads me to suspect that there is an IR presence detector within the lavatory that affects the door behaviour.

⚡ Car won't start if payments are delinquent

"Daniel P. B. Smith" <dpbsmith@world.std.com>

Sat, 14 Aug 1999 12:01:29 -0400 (EDT)

The Boston Globe, 14 Aug 1999, p.3, carries an AP story. A Detroit auto dealer sold cars to people with bad credit containing "a high-tech dashboard device that prevents cars from starting if the customer is delinquent on payments." The story says that "customers get a six-digit code when they pay their bills every week. If they punch the proper code into the device, the car can be started. If more than a week passes without a new code, the car will not start."

Two customers contend that the "On-Time Device" shut off their cars while driving and are suing.

The RISK here is that computer technology is enabling the invention and rapid proliferation of new machinery which is intended to directly and physically enforce policy. From a technical standpoint, the device is not very different from the aftermarket antitheft device I installed on my own car, which similarly a) uses digital technology, and b) interferes with the starting circuits. I worry about its reliability, of course. The big difference is that an ignition lock malfunction puts the purchaser at risk, so presumably market forces would work to insure reliability. The

"On-Time Device" puts someone other than the device's purchaser at risk.

Daniel P. B. Smith <dpbsmith@world.std.com>

★ Salary payment diskettes intercepted and manipulated

Peter Fokker <peter@fokker.demon.nl>

Fri, 06 Aug 1999 06:32:34 +0100 (CET)

My local newspaper (NRC/Handelsblad, 5 August 1999) reports about a successful way to steal money by intercepting diskettes with payment information that are sent - by mail or via a courier service - to the bank subsidiary (Interpay) that handles this kind of payments for all banks here in The Netherlands.

The intercepted diskettes were "cracked" and the swindlers changed one or more destination bank account numbers and amounts, "repaired" the diskettes and sent them to Interpay as if nothing happened.

Some twenty people have been arrested. The damages, "a few million NLG" (1 USD = 2 NLG), for the bank's customers have been compensated by the bank. It is unclear where the diskettes were intercepted (NL Postal services, the courier or within Interpay). Interpay and the combined banks have announced measures for better protection of these diskettes and the transportation thereof.

The RISKS are obvious. I would say: be very concerned when

someone tells you
that "the cheque is in the mail".

--Peter Fokker

⚡ Risks of Internet Explorer 5

Lloyd Wood <L.Wood@surrey.ac.uk>
Fri, 6 Aug 1999 16:09:51 +0100 (BST)

<http://msdn.microsoft.com/workshop/essentials/versions/ICPIE5.asp>

To pick one example from that page:

AutoComplete speeds the collection of demographic information by making it easier to fill out online forms. AutoComplete provides a drop-down list of items that the user has previously entered in a particular text box on a Web page. When the user selects the item, it is automatically put into the field (except for password fields).

The feature is very useful on its own, but its real power shines through when the benefit is transferred between Web sites. Once you mark your input tags with AutoComplete attributes, your users won't have to retype common elements -- such as names, telephone numbers, and e-mail addresses -- because they will have already filled in this information on someone else's site. Internet Explorer stores the form field entries in a secure, client-side store.

1. Don't let anyone else use Internet Explorer 5 on your machine. They might get ideas when filling in forms, and use your personal information instead of typing in their own.
2. client-side is not necessarily secure, as has been previously demonstrated many times.
3. This assumes that password fields are indicated as such; a risk in itself.

<L.Wood@surrey.ac.uk>PGP<<http://www.ee.surrey.ac.uk/Personal/L.Wood/>>

⚡ Refrigerator gasket frozen out

<TED_LEE@udlp.com>

Wed, 11 Aug 1999 08:32:00 -0500

Seeing the item in [RISKS-20.53](#) about a cellphone endangering a plane reminded me of a recent incident that gave me pause to realize that sometimes people may take reasonable precautions. The magnetic gasket on our refrigerator is wearing out so I called around the local appliance parts shops to find one. It turns out that even though (or perhaps because) it is a major brand, there are so many variations they aren't stocked locally (Minneapolis) and it had to be shipped from a Chicago warehouse. I was told I did **not** have the option of air freight or express: it had to go surface because it was regarded as hazardous cargo. I assume that is because it is essentially one big magnet that there is concern it might interfere with

navigation -- but does anyone actually know of an incident or two that might have given rise to that concern? After all, modern planes don't use magnetic compasses anymore, it ain't *that* strong a magnet, and I can't think that its motion in the belly of the plane would generate strong enough radio waves to be of concern.

Ted Lee

✶ Y2K upgrade went 'horribly wrong', admits utility giant

"Edelson, Doneel" <doneeledelson@aciins.com>

Thu, 12 Aug 1999 16:55:51 -0400

London Electricity has admitted its Y2K upgrade for 400,000 prepayment customers (costing 2 million pounds) went ``horribly wrong'', leaving 2000 customers without power and light for days, and another 2000 having ``difficulties''. The process of providing new Rechargeable Powerkeys to customers was in progress, but for a fourth of the clients the payment credit did not get transferred or their meters were corrupted. A similar upgrade in Sussex was done at the same time, which compounded the problems.
[Source: Mike Simons, *Computer Weekly News*, 12 August 1999; PGN-ed]

✶ Government: Lessening risks through encryption

Alan DeKok <aland@striker.ottawa.on.ca>

Tue, 10 Aug 1999 08:50:50 -0400

This is one of the happier risks related items I've seen in a while. The local provincial government has actually *recommended* the use of encryption to secure e-mail.

<http://www.wired.com/news/news/politics/story/21140.html>

While the US Congress recoils in horror at the prospect of a population armed with cryptographic tools, a government department in

Ontario wants to make it clear that encryption is good.

More than that, in a paper released Thursday, the Ontario Information

and Privacy Commission said it wants everyone to learn to use encryption.

The paper is available at:

http://www.ipc.on.ca/Web_site.ups/MATTERS/SUM_PAP/PAPERS/encrypt.htm

Some good quotes from the Introduction:

Does it really matter who reads your e-mails? If the answer is no,

then e-mail encryption could be a potentially cumbersome luxury. However, if you e-mail sensitive, personal, or business

information, then encryption is likely a necessity. [...]

Those people who use some form of encryption system relax comfortably

at their keyboards. Nonetheless, they feel a cold chill each time

someone reports a new security hole. Some holes are found in the

encryption tools. More often though, the application that uses the

encryption tool has bugs. Internet browser applications are prone to

this due to their large size and complexity. While the cryptographic component might remain secure, back door bugs to the application can nullify the value of the e-mail encryption.

⚡ Having private services such as voicemail on shared phones

David Crooke <dave@dcc.vu>
Sat, 07 Aug 1999 00:03:09 -0500

Many hotels now offer phones in rooms with services such as voicemail. I checked into one such establishment recently, and was surprised to find a message already waiting as I always use a mobile phone when travelling.

Needless to say, the message turned out to be for someone else, presumably the previous occupant, and was somewhat (ahem) personal in content, and I hastily deleted it.

When I returned the following evening the message light was on again, the voicemail software having seemingly requeued the message. This went on all week, and I presume will be causing blushes for some time.

David Crooke, Austin TX, USA. +1 (512) 656 6102
"Open source software - with no walls and fences, who needs Windows and Gates?"

⚡ Re: NCIC 2000 (Fenner, [RISKS-20.53](#))

Stephen Fairfax <fairfax@mtechnology.net>

Thu, 12 Aug 1999 19:39:12 -0400

>5) One wonders how long it will be until this system will be used as a
>method of collecting and storing fingerprints on citizens not convicted--or
>even charged with--any crime.

That particular RISK predates the NCIC 2000 system.

A Massachusetts law effective October, 1998 requires all owners of firearms

to report to their local police stations for full 10-print fingerprints and

digital mug shots. The fingerprints and mug shots are forwarded (by law)

to the Criminal History Systems Board. This agency "serves as the hub for

information services for the law enforcement and criminal justice communities." (see [http://www.magnet.state.ma.us/chsb/about.](http://www.magnet.state.ma.us/chsb/about.htm)

[htm](http://www.magnet.state.ma.us/chsb/about.htm)) The same

agency provides access to the FBI NCIC and to all 49 state criminal justice

databases. While the web page does not go into details, does any long time

RISKS reader doubt that the access is reciprocal? What are the RISKS

associated with having the de facto equivalent of a criminal record?

What is particularly ironic about the new licensing requirement is that

(legal) firearms ownership has long been limited to those persons who have

no criminal record. Thus, the statute mandates the collection and

dissemination of fingerprints from people who are known to have committed no crime.

Stephen Fairfax <fairfax@mtechnology.net>

✈ Computers, Freedom, and Privacy: CFP for CFP

Bruce R Koball <bkoball@well.com>

Thu, 12 Aug 1999 13:48:26 -0700 (PDT)

The Tenth Conference on Computers Freedom and Privacy

CFP2000: CHALLENGING THE ASSUMPTIONS

<http://www.cfp2000.org>

The Westin Harbour Castle Hotel

Toronto, Ontario, Canada

April 4-7, 2000

The Program Committee of the Tenth Conference on Computers, Freedom, and Privacy (CFP2000) is seeking proposals for conference sessions and speakers.

We are seeking proposals for tutorials, plenary sessions, workshops, and birds-of-a-feather sessions. We are also seeking suggestions for speakers and topics. Sessions should present a wide range of thinking on a topic by including speakers from different viewpoints. Complete submission instructions appear on the CFP2000 web site at <http://www.cfp2000.org/submissions/>. All submissions must be received by October 15, 1999. The CFP2000 Program Committee will notify submitters of the status of their proposals by December 3.

Workshop on Freedom and Privacy by Design (first day of CFP 2000)
Complete submission instructions are available at <http://www.cfp2000.org/workshop/>

Program Chair: Lorrie Cranor, AT&T Labs-Research

FOR MORE INFORMATION VISIT <http://www.cfp2000.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 20: Issue 55

Friday 27 August 1999

Contents

- [New Microsoft Java flaw](#)
[Edward W. Felten](#)
- [Internet Explorer cannot read \[www.microsoft.com\]\(#\)](#)
[Keith Edmunds](#)
- [Tokyo traffic chaos in GPS date rollover](#)
[Mike Martin](#)
- [GPS rollover hits yacht](#)
[Justin Mason](#)
- [9/9/99](#)
[Lindsay Marshall](#)
- [Y2K in China](#)
[David Cowhig via Donald B. Wagner](#)
- [Downtown Chicago hit by electrical blackout](#)
[Doneel Edelson](#)
- [Power coming back on causes UPS to lose power](#)
[Ray Todd Stevens](#)
- [Numeric pager sending alpha messages](#)
[Ray Todd Stevens](#)
- [Ohio town law against cell phones while driving](#)
[Jim Griffith](#)

- [Justice seeks wider access to computer data](#)
[NewsScan](#)
 - [Inadvertent nameserver cache poisoning](#)
[Rich Lafferty](#)
 - [Purchase circles and insider information](#)
[Joseph A. Dellinger](#)
 - [Can Linux survive software patents?](#)
[Martin Minow](#)
 - [Canadian spy secrets leak on Web](#)
[David Kennedy](#)
 - [Auto-Fix feature for Dell PCs](#)
[Henry Robertson](#)
 - [Re: Car won't start if payments are delinquent](#)
[Keith Edmunds](#)
 - [gnu touch has an unusual sense of time](#)
[B. Elijah Griffin](#)
 - [Security check powers up computer](#)
[Edward Holden](#)
 - [Re: NCIC 2000](#)
[Otto Stolz](#)
 - [USENIX Annual Conference 2000, Announcement and Call For Papers](#)
[Moun Chau](#)
 - [USENIX Security Symposium 2000, Announcement and Call for Papers](#)
[Moun Chau](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **New Microsoft Java flaw**

"Edward W. Felten" <felten@CS.Princeton.EDU>

Thu, 26 Aug 1999 19:51:37 -0400

We have discovered a serious security flaw in the versions of Microsoft's Java Virtual Machine that are distributed with Internet Explorer 4 and Internet Explorer 5 for Microsoft Windows. The flaw allows the

creation of a malicious applet that is attached to a HTML page, which could be delivered over the Web via Internet Explorer or by e-mail via Outlook or other mail programs that use Microsoft's Java Virtual Machine. When the malicious applet is executed, it can read, modify, or destroy any data on the computer, insert a virus, insert software to spy on the user's future on-line activities, or take any other malicious action. The attack does not require the user to do anything beyond viewing the Web page or e-mail message.

The flaw is a programming error (a race condition) in one of the security-critical parts of Microsoft's Java class libraries. A malicious applet can exploit this error to violate Java's security rules. The applet can then proceed to take control of the machine and perform any actions it likes. We have implemented and tested an applet that demonstrates this flaw by deleting a file on the victim's PC.

We are not releasing the demonstration applet or any further technical details about the flaw at this time.

After consultation with us, Microsoft has issued a new version of their Virtual Machine that fixes this problem. A security bulletin from Microsoft can be found at <http://www.microsoft.com/Security/Bulletins/ms99-031.asp>.

For further information, contact Edward Felten at <felten@cs.princeton.edu>, 609-258-5906, or Teresa Lunt at <tlunt@parc.xerox.com>, 650-812-4424.

Edward Felten, Princeton University
Drew Dean, Xerox PARC
Dan Wallach, Rice University
Dirk Balfanz, Princeton University / Xerox PARC

⚡ Internet Explorer cannot read www.microsoft.com

"Edmunds, Keith" <KEdmunds@eu.wcom.net>
Fri, 27 Aug 1999 16:24:03 +0100

I recently installed NT Server 4.0. Before upgrading to Service Pack 5, I wanted to download some third party drivers. NT4 comes with Internet Explorer V2, which is dated to say the least. I first decided to visit Microsoft's web site to upgrade IE2 to IE4 or IE5. However, IE2 refuses to display the home page at www.microsoft.com, giving instead the following message: "Unable to open <http://www.microsoft.com/>. You do not have permission to open this item. Directory Listing Denied This Virtual Directory does not allow contents to be listed."

The RISK here is obvious. Ensure that your web site can be read by old browsers, even if it isn't very pretty. This is particularly so if your current product (NT 4.0) includes an obsolete browser itself...

Keith Edmunds Reading UK <edmunds@itworks.demon.co.uk>

⚡ Tokyo traffic chaos in GPS date rollover

"Martin, Mike" <mmartin@sbns.com.au>

Tue, 24 Aug 1999 10:55:20 +1000

The Australian Financial Review's Tokyo correspondent, Andrew Cornell, reports (AFR Aug 24) that the GPS date rollover, previously discussed at length in RISKS, occurred at 9 am Sunday Aug 22 in Japan and that "an estimated 100,000 systems", mainly used by vehicle drivers for navigation through Tokyo's unnamed streets, "froze or went blank as the system rolled over into its new time sequence".

Cornell reports that Pioneer, the GPS market leader, had been advertising to notify customers of the problem, and had adapted or replaced 210,000 of its 270,000 affected systems.

If this incident is typical of consumers' and small businesses' response to a technology brick wall then it does not bode especially well for January 1 next year.

Mike Martin

[See also Reuters, *The New York Times*, 23 Aug 1999, <http://www.nytimes.com/library/tech/99/08/biztech/articles/23gps.html/> PGN]

GPS rollover hits yacht

Justin Mason <jm@netnoteinc.com>

Sun, 22 Aug 1999 20:01:15 +0100

From this evening's RTE news:

The Irish Marine Emergency Service has been dealing with a yacht on route from the Scilly Isles to Kinsale which ran into fog and heavy weather south of Ireland this morning. Local reports say that "The Tam-o-Shanter" radioed for help when its Global Positioning System began to misread the boat's position. The crew were further hampered by extremely heavy weather and a torn sail. With the aid of the IMES and Coast Radio Stations, a position was given and the yacht is now safely in Kinsale Harbour.

It is believed a millennium style bug caused the "Tam-o-Shanter" to lose its position today. At midnight GMT (1am Irish time) the GPS "rolled over". After its launch in 1980 it had a life span of 1,024 weeks, which reached zero this morning when the system reverted back to its start time. All mariners had been warned of this, but GPS units older than five years would not have been capable of handling the change.

(snipped from <http://www.rte.ie/news/1999/0822/boys.html>)

9/9/99

<Lindsay.Marshall@newcastle.ac.uk>

Mon, 23 Aug 1999 11:43:03 +0100 (GMT)

According to a report in one of the UK Sunday papers two real occurrences of the fabled 9/9/99 bug have been found, one in a non-critical medical application. It would be interesting to have more information

about this as

I have always thought that the 9/9/99 bug sounded like press scaremongering rather than something that would really arise.

<http://catless.ncl.ac.uk/Lindsay>

Y2K in China

"Donald B. Wagner" <dbwagner@coco.ihiku.dk>

Mon, 23 Aug 1999 09:31:45 +0200

Date: Sat, 21 Aug 1999 20:32:39 -0400

Reply-To: H-Net list for Asian History and Culture <H-ASIA@H-NET.MSU.EDU>

From: David Cowhig <dcowhig@public3.bta.net.cn>

Subject: H-ASIA: May 1999 China Y2K National Conference: Guarded Optimism

May 1999 China Y2K National Conference: Guarded Optimism A June 1999 report
from U.S. Embassy Beijing

<http://www.usembassy-china.gov/english/sandt/Y2kcnfwb.htm>

[see also the recently updated links to Chinese Y2K related websites at

<http://www.usembassy-china.gov/english/sandt/y2gov.htm>]

Summary: China Y2K Czar Zhang Qi and other speakers at the Second PRC

National Y2K Conference held on May 6-7 in Beijing expressed greater

confidence in China's electric power grids but greater concerns about the

effect of the Year 2000 computer problem on railroad freight, medical

instrumentation and embedded chips. Zhang Qi said that electric power

companies would be assured funding for Y2K solutions. Some

Chinese experts

doubt, however, that Y2K funding will be made available; the August 1998

State Council Y2K order made each unit responsible for funding its own Y2K

solutions. Zhang mentioned the recent Shanghai Y2K Seminar with Secretary of

Commerce Daley and her upcoming August 1999 USIA sponsored trip to the

U.S.A.. Central government speakers discussed the Y2K problem in telecommunications, electric power, and transportation. Local government and

industry Y2K speakers came from Liaoning Province, Beijing Municipality, the

Beijing Municipal Health Bureau, the Baoshan steel company and Chinese

banks. Two speakers discussed Y2K legal liability issues. The speakers

agreed that China faces Y2K difficulties in many sectors but no one foresaw

a national cataclysm. The Embassy Beijing view is that Y2K will not put

American citizens in China into danger but will likely affect business and

especially small businesses such as suppliers and small contractors. These

Y2K problems might affect the overall Chinese economy gradually over weeks

and months.

⚡ Downtown Chicago hit by electrical blackout

"Edelson, Doneel" <doneeledelson@aciins.com>

Thu, 12 Aug 1999 16:32:30 -0400

Downtown Chicago experienced extensive blackouts on 12 August 1999.

Initially, three of the four transformers at a North Side substation went

off-line. (One transformer had been undergoing repairs.) In

addition, a high-voltage cable failed. This caused Commonwealth Edison to black out about 2300 customers in two different areas. The Chicago Board of Trade, other exchanges, banks, businesses, and residences were shut down. [Reuters item, forwarded by Doneel from Yahoo! News Top Stories Headlines, 12 August; PGN-ed]

⚡ Power coming back on causes UPS to lose power

"Ray Todd Stevens" <raytodd@kiva.net>

Mon, 23 Aug 1999 20:03:41 +0000

This is an interesting failure mode. Situation: Computer (monitor and printer) running on a UPS that is plugged into 110 with other items. Here is the failure sequence.

Power goes out for a period of several minutes (at least 15 to cause failure) UPS has been sized to allow 1 hour run time for computer.

Everything runs fine. User acknowledges the UPS alarm and continues to work

as planned. Power is restored. Everyone assumes that all is OK. UPS

switches into battery charge mode and switches to line mode.

The combined

load is more than the breaker can take. Now we have a localized power failure.

#1 The power is back for such a short duration that the alarm on the UPS doesn't reset and trigger.

#2 The other items on the circuit are noncritical and are not noticed to be off line.

So, after about 30-45 minutes, the computer crashes with no warning.

Ray Todd Stevens, Senior Consultant, Stevens Services
R.R.#14 Box 1400, Bedford, IN 47421 (812) 279-9394
Raytodd@tima.com

⚡ Numeric pager sending alpha messages

"Ray Todd Stevens" <raytodd@kiva.net>
Mon, 23 Aug 1999 20:05:19 +0000

One of my friends works in the customer service call center of a national pager company. He deals with the usual complaints regarding poor pager operation, as well as the occasional crank caller demanding to be paged less often, more often, or by more interesting people.

The best call came from a man who repeatedly complained that he keeps being paged by "Lucille." He was instructed that he would have to call her and tell her to stop paging him.

"She don't never leave no number, so I can't call her back," he said.

After three such calls, someone thought to ask how he knew it was Lucille if she didn't leave a number.

"She leaves her name," was the reply.

After establishing that the customer had a numeric-only pager,

the light
bulb came on.

"How does she spell her name?" the service rep asked.

"L-O-W C-E-L-L"

Another problem solved.

[I picked this up off of a joke list, but it certainly seems
to apply to
this list also.]

Ray Todd Stevens, Senior Consultant, Stevens Services
R.R.#14 Box 1400, Bedford, IN 47421 (812) 279-9394
Raytodd@tima.com

🔥 Ohio town law against cell phones while driving

Jim Griffith <griffith@netcom.com>
Wed, 25 Aug 1999 16:17:00 -0700 (PDT)

CNN reports that Brooklyn, Ohio has passed a city ordinance
banning the use
of all but hands-free cell phones in moving vehicles, except in
emergency
situations. Effective September 1, violations may result in a
\$100 fine.
The city is responding to recent studies that show that the
chance of having
an accident dramatically increases (one study says "quadruples")
when cell
phones are being used.

<http://www.cnn.com/US/9908/25/cellphone.ban/>

Justice seeks wider access to computer data

"NewsScan" <newsscan@newsscan.com>

Fri, 20 Aug 1999 08:20:25 -0700

The Justice Department wants to broaden rules for allowing law enforcement officials to secretly enter suspects' homes or offices and disable security on PCs in advance of administering a wiretap or conducting a further search.

An Aug. 4 memo says that encryption software "is increasingly used as a means to facilitate criminal activity, such as drug trafficking, terrorism, white-collar crime, and the distribution of child pornography." Officials at the Justice Department have drafted the Cyberspace Electronic Security Act, which would expand existing search warrant powers to allow for disabling encryption. To extract information from the computer, agents would still be required to get additional authorization from the court.

Privacy advocates say the proposed legislation would compromise personal freedoms: "They have taken the cyberspace issue and are using it as justification for invading the home," says a spokesman for the Center for Democracy and Technology. [**The Washington Post, 20 Aug 1999**, <http://www.washingtonpost.com/wp-srv/business/daily/aug99/encryption20.htm>;

NewsScan Daily, 20 August 1999; reproduced with permission. To subscribe to NewsScan Daily, send an e-mail message to NewsScan@NewsScan.com with 'subscribe' in the subject line.]

✶ Inadvertent nameserver cache poisoning

Rich Lafferty <rich@alcor.concordia.ca>

Mon, 23 Aug 1999 02:51:02 -0400

[Site names omitted to protect the guilty and innocent...--r]

I just ended an unusual conversation in which myself and a colleague were enlisted to help debug a nameserver problem in which, according to the original report, a large site had started using a smaller site's nameservers for all its requests.

As it turns out -- and the nature of the original report, pointing at the large site, managed to disguise this for a while -- the smaller site was a domain farm, where, instead of adding A records for their thousands of domains and hundreds of hostnames in each domain, they had configured their nameserver to respond with a particular A record for any responses that managed to make it to their nameserver. While this would also give their address to queries for names that they weren't authoritative for, this wasn't a problem in practice, as they had no local users using those nameservers.

In other words, when working, only queries regarding their domains would reach their server, and their server would respond with the same address for all of those. Not particularly elegant, but it seemed to work.

Then they added NS records to those responses. And not just any NS records -- accidentally or otherwise, all of their responses were

claiming NS
authority over .com.

Now, usually, that wouldn't get picked up by anyone --
nameservers querying
their server would have a perfectly-good cached NS record for .
com. obtained
from a root nameserver. But it *did* happen that the nameserver
at this
large site managed to start thinking that this little nameserver
was
responsible for .com., and started sending all of its queries
there. As far
as I can tell, it was only a matter of unfortunate timing, with
a request
landing at that server and their cached NS record for .com.
expiring at
nearly the same time.

The effects were somewhat disastrous, of course. Since the
nameserver was
configured to give the same A record for everything, all of the
requests for
*.com from the large site ended up at the same page full of
advertisements. The domain servers at the small site were
overwhelmed, and
so were the *web* servers, having to serve up the page full of
adverts so
often.

While nameserver cache poisoning is something of an old RISK,
this instance
had unusual repercussions in that it basically ended up with a
denial of
service for all parties involved. (While we hope we caught it
before it
became an extended problem, had we not, it would have continued
indefinitely
as the small site's nameserver continued reminding the large
site that it
was responsible for .com. with every request any of the large
site's clients
might have made.)

(Interestingly, it took some explaining before the small site would acknowledge that the problem was at their end -- it often comes as a surprise to small Internet quick-buck operations such as these that what they do wrong can have such a disastrous effect on other parties. The ones described above ended up getting things resolved after encountering myself and a colleague on an IRC channel which offers help with Unix.)

Rich Lafferty, Information and Instructional Technology
Services, Concordia
University, Montreal, QC 1-514-848-7625 rich@alcor.concordia.ca

✶ Purchase circles and insider information

"Joseph A. Dellinger" <jdellinger@amoco.com>
Thu, 26 Aug 1999 15:54:23 -0500 (CDT)

Amazon.com has come out with a new service, "purchase circles". It lets you look up the 10 most popular books ordered by people at different companies. I'm not sure amazon.com realizes how powerful an information source this is. I heard about this new feature from Stanford students near graduation, who are using it to assess the relative "Dilbert index" of possible future employers (as indicated by the ratio of new-age management to technical books making the list). You can also use it to get some idea of the current mood within a company. One large oil company in particular stands out: people there are mostly ordering books on changing careers and on introductory web/programming/internet skills. Not

surprisingly, this is a company about to be acquired.

The complete list of books being ordered by a given company might provide very interesting insider information. There might be a noticeable spike in "What color is my parachute" orders preceding public disclosure of an impending big layoff, for example. A rash of "introductory Spanish" book orders might indicate a planned expansion into or relocation of workers to a Spanish-speaking country. How long before employees are ordered not to order books over the internet using their work accounts?

⚡ Can Linux survive software patents?

Martin Minow <minow@pobox.com>
Sun, 15 Aug 1999 21:14:30 -0700

<<http://linuxjournal.com:82/articles/currents/003.html>>

An interesting article on the effect of patents on open source software.

Disclaimer: I'm a co-author of one patent, and recently authored three software patents for my former employer.

Before moving to San Francisco, I helped a friend try to recover backup tapes from MIT-AI (the birthplace of the Open Source movement, though there was much open source available before that computer). It seems that MIT folk wanted to recover "prior art" (from the 1960's) that is now being patented.

Martin Minow minow@pobox.com

✶ Canadian spy secrets leak on Web

David Kennedy CISSP <dmkennedy@compuserve.com>

Fri, 27 Aug 1999 02:32:39 -0400

<http://www.globeandmail.com/gam/National/19990826/USPYYN.html>

by Andrew Mitrovica

>In what intelligence experts are calling an embarrassing gaffe and a

>serious breach of security, one of the military's top-secret electronic

>eavesdroppers posted the names and location of CF-18 pilots based in Italy

>on his own Web page before and during the war in Yugoslavia, The Globe and

>Mail has learned. [...]

>Moreover, he said he set up his Web page with the consent of his superiors

>at the Defence Department before he shut it down in the spring because he

>feared that it might imperil the lives of CF-18 pilots and their crews, who

>made hundreds of bombing sorties during the Balkans war. [...]

>Reg Whitaker, a York University political science professor and an expert

>on intelligence matters, said MCpl. Arsenault's Web page was "a very

>serious breach of security. And it clearly provides confirmation that these

>guys [CSE] were there [in Italy]. It's safe to assume that this kind of

>sensitive information being posted on the Internet is not

official policy

>for the agency. That's really very embarrassing." [...]

>His Web page was not the only source of information about
military snoops

>and the CSE to appear on the Internet recently.

>

>In March of 1997, the Defence Department briefly posted on its
own Web site

>confidential information about military personnel who collect
and monitor

>communications for the CSE, known in the military as "291ers."

>

>The department's Web site provided a complete list of the
number, location,

>rank and responsibilities of hundreds of researchers throughout
Canada, the

>United States and Britain. However, it did not include names.

Dave Kennedy CISSP Director of Research Services ICSA.net

<http://www.icsa.net>

⚡ Auto-Fix feature for Dell PCs

"Henry Robertson" <robertsn@jlab.org>

Thu, 26 Aug 1999 09:34:48 -0400

These days many people (not me) have gotten used to the auto-
update features

for various software packages. For example, the Norton Antivirus
program can

be set so that every Friday night it automatically connects to
the Norton

web site and downloads the latest virus protection features. Not
a bad idea

if you trust this type of connection. Well, Dell has taken this
a bit

further. A product called "Open Manage Resolution Assistant"
will reside on

their next series of servers/workstations. It looks for failures

or errors
and auto-notifies Dell's technical staff. (The worst is yet to
come.) Dell's
staff then has the capability of doing remote diagnostics and
running
certain "scripts" on your computer to find the problem. This
requires a
major hole in your system firewall! If you feel comfortable with
a
technician in Texas roaming around on your financial server,
then this isn't
as scary for you as it is for me.

For more info see "Inter@ctive" magazine, vol.6, no.34, page 7.

Henry Robertson, Safety Systems Group, Jefferson Lab
robertsn@jlab.org 1-757-269-7285

✶ Re: Car won't start if payments are delinquent (Smith, [RISKS-20.54](#))

"Edmunds, Keith" <KEdmunds@eu.wcom.net>

Fri, 27 Aug 1999 16:02:39 +0100

> ...The big difference is that an ignition lock malfunction
puts the
> purchaser at risk, so presumably market forces would work to
insure
> reliability."

Insure or ensure? "Insure" means you accept that the risk exists
and ask
someone else to pay out in some way if the risk is realised;
"ensure" means
you do everything you need to do to remove the risk.

The RISK here is a misunderstanding about whether or not the
risk exists,
and what comeback there might be if it does. Perhaps the real

risk is not
understanding the difference between American and English: as
one person
once said, "Two nations divided by a common language."

Keith Edmunds Reading England <edmunds@itworks.demon.co.uk>

✶ gnu touch has an unusual sense of time

"B. Elijah Griffin" <eli@panix.com>

Fri, 27 Aug 1999 16:59:09 -0400 (EDT)

Today I was trying to use the output of "ls -l" and the --date
option of
touch (from GNU fileutils 4.0) to restore time stamps on some
files I'd
ftp'd to something close to the original time stamps.

Apparently, however, a command like:

```
touch --date='Nov 11 1996' file
```

results in "1996" being interpreted as 7pm plus 96 minutes or
8:36pm, which
I find to be a distinctly non-intuitive understanding of time.

Had I not double-checked the results, these mistaken time stamps
would have
remained and conflicted with my intent for restoring them in the
first
place.

Elijah

Of course, ls's ideas about displaying time are screwy enough.

[Of course, "fileutils" looks like it might be a French word
if you treat the "eu" as a diphthong. But then a diff-thong
might be
a program that discriminates between things like thongs and

songs. PGN]

✈ Security check powers up computer

<eholden@ix.netcom.com>

Tue, 24 Aug 1999 08:22:45 -0400

Before flying I normally put my laptop computer in my carry-on bag in standby mode, where the contents of memory are stored on the hard disk and the power is off.

Perhaps a dozen times in six months, the procedure for inspecting bags on entry to the terminal seems to have managed to restart the computer. An hour into flight, I discover the computer is on and the battery is 80% used. This is irritating(!) and perhaps dangerous, although none of my flights has crashed.

Sometimes, now, I remember to check the machine is still power-off by inspecting it after boarding the plane while still parked at the gate. On one such occasion I was strongly reprimanded by a flight attendant for "using" the computer at that time.

I find it interesting that an anti-terrorist inspection might risk creating an electronic hazard to a flight.

Edward Holden

✶ Re: NCIC 2000 (Fairfax, [RISKS-20.54](#))

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

Mon, 23 Aug 1999 10:17:38 -0600

> What is particularly ironic about the new licensing
requirement is that
> (legal) firearms ownership has long been limited to those
persons who have
> no criminal record. Thus, the statute mandates the collection
and
> dissemination of fingerprints from people who are known to
have committed
> no crime.

Rather, those fingerprints are collected from people who are not
known
to have committed a crime -- an essential difference, and
probably part
of the rationale for that statute.

Otto Stolz

✶ USENIX Annual Conference 2000, Announcement and Call For Papers

Moun Chau <moun@usenix.ORG>

Fri, 27 Aug 1999 19:57:52 GMT

2000 USENIX Annual Technical Conference

June 18-23, 2000

San Diego Marriott Hotel & Marina

San Diego, California, USA

<http://www.usenix.org/events/usenix2000>

Sponsored by USENIX, the Advanced Computing Systems Association.

Please see the detailed submission guidelines and conference
information: <http://www.usenix.org/events/usenix2000/cfp>

Paper Submissions deadline: November 29, 1999

✦ USENIX Security Symposium 2000, Announcement and Call for Papers

Moun Chau <moun@usenix.ORG>

Tue, 24 Aug 1999 20:00:31 GMT

9th USENIX Security Symposium 2000 Conference

August 14 - 17, 2000

Denver, Colorado, USA

Conference URL: <http://www.usenix.org/events/sec2000>

The USENIX Security Symposium brings together researchers, practitioners, system administrators, systems programmers, and others interested in the latest advances in security and applications of cryptography. The keynote speaker is Dr. Blaine Burnham, Director of the Georgia Tech Information Security Center (GTISC) and formerly Program Manager for the National Security Agency (NSA) at Ft. Meade, Maryland.

See

<http://www.usenix.org/events/sec2000/cfp/guidelines.html>

Paper submissions due: February 10, 2000

[Wow! A year from now, and I just got back last night from the 1999

Conference in WashDC, after sitting on the plane docked at the gate

at Dulles, which finally took off four hours late while we waited

for a bunch of storms to pass. At least I did not have to go through

Chicago, where most UAL flights were cancelled because of someone

who evaded the security controls. 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 20: Issue 56

Friday 3 September 1999

Contents

- [Online gambling software flaw](#)
[Matthew Schmid](#)
- [Test page for dangerous ActiveX controls](#)
[Richard M. Smith](#)
- [Intuit strikes again](#)
[Gary Cattarin](#)
- [Danish UPS](#)
[Finn Jensen in rec.humor.funny](#)
- [Tandy bug?](#)
[Lindsay Marshall](#)
- [E*Trade and the Dow Jones](#)
[Theodore Y. Ts'o](#)
- [U.S. top-secret messages go astray](#)
[Andrew Johnson](#)
- [UPenn bug report](#)
[Rebecca Mercuri](#)
- [Local company stung by Y2K bug](#)
[Doneel Edelson](#)
- [Smart Card Forum annual meeting](#)
[Donna Farmer](#)

● [Info on RISKS \(comp.risks\)](#)

✶ Online gambling software flaw

"Matthew Schmid" <mschmid@rstcorp.com>

Fri, 3 Sep 1999 05:26:02 -0700 (PDT)

Regardless of its quasi-legal status, online gambling presents an entire raft of risks. Key questions include: Will your personal information be handled securely (for example, will the credit card number you're paying with be stolen or the fact that you're gambling at all be leaked)? What if the gaming site is hacked? Could you be playing against cheating insiders or players acting in collusion? Are the games implemented correctly and fairly? Is the software secure? In response to the last question, we have demonstrated that the answer is no.

The Software Security Group at Reliable Software Technologies (www.rstcorp.com) has discovered a serious flaw in the implementation of Texas Hold 'em Poker that is distributed by ASF Software, Inc. (www.asfgames.com). We have exploited this flaw in the lab. Our exploit allows a player (us) to calculate the exact deck being used for each hand in real time. That means a player using our exploit knows the cards in every opponent's hand as well as the cards that will make up the flop (cards placed face up on the table after rounds of betting). We can win every time. A malicious attacker could use our exploit to bilk innocent players of actual money without ever being caught. ASF Software has

been notified
of the flaw.

Currently we know of three online casinos (www.planetpoker.com,
www.purepoker.com, and www.deltacasino.com) that appear to use
ASF

Software's implementation of Texas Hold 'em Poker. All three
Websites allow
players to compete for real money. There is also a demo casino
(www.casinococo.com) that allows players to gamble with play
money. We have
only used our exploit against the demo casino.

The flaw exists in the card shuffling algorithm used to generate
each deck.

Ironically, the code was publicly displayed at www.planetpoker.com/ppfaq.htm

with the idea of showing how fair the game is to interested
players (the

page has since been taken down). In the code, a call to
`randomize()` is

included to produce a random deck before each deck is
generated. The

implementation, built with Delphi 4 (a Pascal IDE), seeds the
random number

generator with the number of milliseconds since midnight
according to the

system clock. That means the output of the random number
generator is easily

predicted. A predictable "random number generator" is a very
serious

security problem.

There are a number of other problems in the implementation that
could lead

to complete security compromise. We have only exploited the
easiest one at

this time.

The broad take-home message from this work is simple: when
software

misbehaves, bad things can happen. Our mission in the Software
Security

Group is to stamp out insecure code before it is placed in service. Members of the group involved with the Gambling exploit are: Brad Arkin, Frank Hill, Scott Marks, Matt Schmid, and TJ Walls. The Software Security Group is led by Dr.Gary McGraw.

Matt Schmid, Reliable Software Technologies <mschmid@rstcorp.com>

⚡ Test page for dangerous ActiveX controls

"Richard M. Smith" <smiths@tiac.net>
Sun, 29 Aug 1999 14:04:32 -0400

There are a number of outstanding problems with ActiveX controls that are awaiting patches from Microsoft. I've put together a test page which will determine which dangerous ActiveX controls are installed on a system. Here is the URL:

<http://www.tiac.net/users/smiths/acctroj/axcheck.htm>

I think the best solution for right now is to turn off ActiveX in IE4 and IE5.

The "bad guys" can use these controls to do all sorts of nasty stuff in Web pages, HTML E-mail messages, and even newsgroup messages. Affected products are Internet Explorer, Outlook, Outlook Express, and Eudora.

Note: the test page requires IE4 or IE5. Netscape users are safe because Navigator does not support ActiveX controls.

Richard

⚡ Intuit strikes again

"Gary Cattarin" <gcattari@nortelnetworks.com>

Wed, 1 Sep 1999 20:54:13 -0700

Intuit blows it again. Should we be surprised?

Go to: <http://privacy.intuit.com/> Read all the high and mighty
"We're so
careful about your privacy it hurts" crap.

At the bottom, find a link that reads, "If you would like to review or change your contact preferences, please click here." Enter your last name and ZIP code. No, wait, enter ANYONE'S last name and ZIP code who you think might use any Intuit product. It's not hard to think of someone who might. Of course, you are taken - without any verification whatsoever - right to that individual's privacy profile, where you can determine your friend's, neighbor's, enemy's, or mother's choice of receiving junk snail mail, e-mail, and/or phone solicitations from Intuit, or whether Intuit may spread their information across the globe (only to "vigorously screened companies" of course!!!). You can even change their e-mail - so perhaps you can use someone else's profile to create SPAM into your favorite enemy's inbox!
(Oh, if Dick Nixon were still alive...)

Risk? Privacy statements and policies mean nothing if the

company maintains
no control over the information required to implement them.
Weak attempts
at "privacy control" allow easy abuse and further multiply the
problem.

So go ahead! Protect your neighbor from junk mail. I did.
(He'd thank me
for it if he ever knew I could do that.)

Gary Cattarin - cattarin@ma.ultranot.com
(Humans will guess the real address - e-mail address-grabbing
scanners will
not!)

Danish UPS

Finn Jensen <f_jensen@mail.tele.dk>

Tue, 31 Aug 1999 19:30:00 PDT

[Courtesy of Aram Khalili, Jim Griffith, and Julian Thomas]

To good to be true, but it is. From the Tele Danmark (ISP)
homepage,
translated from Danish.

>This morning, Tele Denmark Internet was out of order, because
the power
>supply failed. It meant that customer couldn't connect to the
Internet.
>
>The problem occu[r]red at 7:45, when a truck drove into the
cabinet that
>supplies Tele Denmark Internet with power. The truck was
delivering a new
>uninterruptible power supply, and therefore the old UPS had
been disconnected.
>At 9:00 the power returned and the different system began to
reestablish, and
>everything is expected to return to normal again by 10:30. Tele

Denmark

>Internet regrets the disturbance to its customers.

[http://www.opasia.dk/online/tele_danmark/index.html, English here cleaned up a bit for humor's sake - ed.]

⚡ Tandy bug?

<Lindsay.Marshall@newcastle.ac.uk>

Fri, 3 Sep 1999 14:09:52 +0100 (GMT)

The following story was recently forwarded to the EGR mailing list. I

wonder if anyone knows anything more about it? L.

2) William Slattery shares the following personal experience.

All you

reporters out there might take special note.

Y2K is here!

I got a check in the mail last week from Tandy Corporation: \$891.24. A nice chunk of change that there is no way in the world

they could owe me.

Here is what I think happened. Because of my odd habit of paying

off most of my bills to the nearest ten dollars OVER what I actually owe (it makes the math easier when I balance my checkbook), I had a small credit on my Radio Shack credit card.

Their computer looked at the end of the billing period, which fell after the infamous 9/9/99, and said Wowza!, this guy has had

a five dollar credit on our books since January 1 of 1900. Since

company policy is to pay off credits on inactive accounts, I'm

going to calculate the interest and cut this guy a check.

So here we are. I phoned Tandy headquarters (817-415-3011) and talked with the person in charge of this sort of thing, Lisa Mapes. I told her there was no way Radio Shack could owe me 900

bucks because I hadn't spent that much money in their stores in my whole life. I told her I thought they had a Y2K problem. She

laughed at me. It was not a good laugh. It was the "you're so ridiculous it's hilarious" kind of laugh. Ms. Mapes told me to go

ahead and cash the check. Radio Shack really owes me this money,

she says, even though they are completely unable to explain WHY

they owe me the dough.

I told reporters at The New York Times and National Public Radio

that all their stories warning about Y2K were finally starting to

pay off. I figured that after years of running Chicken Little stories -- the sky is gonna fall! the sky is gonna fall! -- it would make a good little story when the first chunks of sky actually started landing on people's heads. Apparently not.

They seem profoundly uninterested.

To a mind as comprehensive as yours, I am sure the potential for

gaining fabulous wealth is immediately apparent. The key to getting rich off Y2K is to open numerous small accounts under assumed names, lodge small credits in them, and wait for the checks to roll in. If I'd thought of it sooner -- and could get

rid of this pesky conscience -- I'd be a rich man today.

E*Trade and the Dow Jones

"Theodore Y. Ts'o" <tytso@mit.edu>

Thu, 2 Sep 1999 16:33:57 -0400

After suffering through the E*Trade / Red Hat fiasco, where each time I talked to a human being, I was really impressed, but each time I had to deal with the web page software I was less than impressed, I suppose I shouldn't be surprised about much from E*Trade's web page.

But imagine my amusement when I looked at E*Trade's main web page, which according to its Market Watch, as of 9/2/1999, at 2:49pm the Dow Jones Industrial Average was \$1.00, down \$10936.88. Somehow, I have a little bit of trouble believing that. Either that, or that stock market bubble that Greenspan keeps worrying about was far more real than anyone ever believed!:-)

(Given that the Nasdaq has only dropped 21.5 points today, I'm assuming the DJIA didn't really lose over ten thousand points.)

Obviously, E*Trade's software doesn't have any "that can't *possibly* be right" checks, so when it somehow got the bogus data about the value of the DJIA, the software very happily calculated that if the index is currently worth one dollar, then it must have dropped \$10,936.88 since yesterday.

Fortunately, it's pretty obvious that the DJIA on the Market Watch web page couldn't possibly be right, but this brings up some obvious questions that should be familiar to all Risks readers: what if some other dumb computer program which was rigged to do program trading decided this

meant it should
dump all of its holdings in a hurry? (Or buy lots of stocks
since obviously
everything is cheap.) What if the numbers on E*Trade's Market
Watch were
off by some significant amount, but not in a way which made it
immediately
obvious that it was in space? Could a human being be taken in
by its a
likely-looking-but-wrong DJIA, and mistakingly make some trades
based an
incorrect market index?

- Ted

P.S. I've saved a copy of the gif image displayed by E*Trade's
Market
Watch, for those who'd like to see this for themselves. It can
be found
at:

<http://web.mit.edu/tytso/www/etrade-djia.gif>

🔥 U.S. top-secret messages go astray

"Andrew Johnson (A.J.)" <johnsy@clear.net.nz>
Fri, 3 Sep 1999 18:30:53 +1200

A common risk inherent in all of our communication technology
is...well,
once again, human error. Next week New Zealand hosts the APEC
conference in
Auckland, being attended by a substantial number of world
leaders, including
President Clinton from the U.S.

So imagine if Saji Phillips, a chicken farmer from Auckland, had
been one of
those people who holds a grudge: He was accidentally faxed the
security

arrangements for the U.S. Embassy and U.S. Delegation, including Mr Clinton, today N.Z. time (3 September 1999).

See Newsroom.co.nz : <http://www.newsroom.co.nz/story.asp?s=5469>

[Another story says this had happened repeatedly.]

The Risk here is very clear... imagine how much that information would be worth to the right person! Not that anyone would think that free trade is a bad thing, of course. *ahem*...

Andrew Johnson <johnsy@clear.net.nz> <http://critique.net.nz/aj/mania/>

UPenn bug report

Rebecca Mercuri <mercuri@gradient.cis.upenn.edu>
Wed, 1 Sep 1999 17:51:43 -0400 (EDT)

Here's the report on what happened to cut Penn entirely off from the Internet. R.Mercuri

Date: Tue, 31 Aug 1999 20:11:25 -0400
Reply-To: Network Administration <netadmin@ISC.UPENN.EDU>
From: Network Administration <netadmin@ISC.UPENN.EDU>
Subject: ****EXTERNAL CONNECTIVITY RESTORED****
Comments: To: pennnet-announce@isc.upenn.edu
To: UUGP@LISTS.UPENN.EDU

Date: Tuesday August 31, 1999
Time: 2:20pm - 7:30pm
Duration: 5 hours
Buildings Affected: Entire Campus
Services Affected: Internet Connectivity
Description: At 2:20 this afternoon, the University's

Internet connectivity was disrupted due to a problem with a Bell Atlantic high-speed line. By 7:30 this evening, Bell Atlantic had taken steps to restore our link to UUNet. There may be a brief interruption to our service in the next 24-48 hours while Bell Atlantic makes permanent repairs.

netadmin@isc.upenn.edu

⚡ Local company stung by Y2K bug

"Edelson, Doneel" <doneeledelson@aciins.com>

Fri, 3 Sep 1999 12:18:36 -0400

Y2K glitches happen to even the most computer savvy folks. Wayne Moule, president of Northwest Metrology, a company that calibrates electronic test equipment for federal agencies and major corporations, is a case in point.

Moule sees the damage every day and still is counting losses - \$80,000 and growing - because software he owns fell victim to a year 2000 problem. ...

[Source: Marc Benjamin, *The Bakersfield Californian*, 24 August 1999;

PGN-ed]

⚡ Smart Card Forum annual meeting

"Donna Farmer" <dfarmer@smartcardforum.org>

Sun, 29 Aug 1999 17:40:30 -0400

Who: Leading privacy and Internet commerce technologists

What: Smart Card Summit '99: Privacy & Security in the New Millennium

When: September 22-23, 1999

Where: JW Marriott Hotel in downtown Washington, DC

Web-information: <http://www.smartcardforum.org> or call (202) 530-5306.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 57

Weds 15 September 1999

Contents

- [Leaving a field blank wipes out 13.2 billion pounds UK](#)
[David Parkinson](#)
- [Dumb computers & the instantaneous nature of e-business](#)
[David Parkinson](#)
- [Smile for the US Secret Service](#)
[Monty Solomon](#)
- [NOAA predicts early winter](#)
[Bill Seurer](#)
- [The real story on Centaur/Milstar](#)
[Peter B. Ladkin](#)
- [If it quacks on 1/1/2000, it must be a Y2K duck](#)
[Win Treese](#)
- [Food expiry date misreading risks](#)
[John Stockton](#)
- [Army dumps NT, moves to Mac](#)
[Martin Minow](#)
- [New Hotmail breach reported](#)
[Keith A Rhodes](#)
- [New ICQ Trojan](#)
[CJNN via Patrick O'Beirne](#)

- [Macro viruses and Word'97's built-in macro detector/disabler](#)
[Gisle Hannemyr](#)
 - [Microsoft Installs US Spy Agency with Windows](#)
[Andrew D. Fernandes](#)
 - [Commentary on Back Orifice](#)
[Bruce Schneier](#)
 - [CPSR Conference: The Internet Gold Rush of '99](#)
[Susan Evoy](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Leaving a field blank wipes out 13.2 billion pounds UK

David Parkinson <dparkins@alien.bt.co.uk>

Thu, 09 Sep 1999 13:28:42 +0100

from *The Times* (London), 9 Sep 1999

Leave one field blank and....

AN INADVERTENT sell order for Vodafone AirTouch sent shares in the heavily weighted mobile telecoms group tumbling and wiped nearly 70 points from a FTSE 100 index that was already reeling from an unexpected UK base rate rise.

A dealer at a US securities house, believed to be Lehman Brothers, entered a massive sell order for Vodafone at 1.40pm. The order is thought to have been set without limits, which meant it matched all bids on the order book and triggered a collapse in the shares from UKP12.29 to UKP10.13.

That sale temporarily wiped UKP13.2 billion from the value of the telecoms giant, which, due to its 6.4 per cent weighting in the FTSE 100, pushed the

blue chip index 66 points lower.

✶ Dumb computers & the instantaneous nature of e-business

David Parkinson <dparkins@alien.bt.co.uk>

Thu, 09 Sep 1999 13:45:17 +0100

Retail outlet Argos ran an add that offered 21-inch Sony Nicam TV sets to Internet customers for 3 pounds instead of 300.pounds. A spokesman for Argos said: "The pricing of the TV sets at UKP3 was clearly an error caused by a computer. We rectified this mistake and we will be contacting our customers to apologise for any inconveniences and explain that their orders cannot be accepted." (One customer had ordered 1,700 sets.) [Source: Adam Fresco, *The Times* (London), 9 Sep 1999; PGN-ed]

Today's (instant?) electronic communication system means you haven't got long to correct mistakes on your e-commerce web site before the word gets out. Also they can be at your door in seconds - even from the other side of the world.

(I'm sure the neighbourhood store would cotton-on at the first transaction, and even the most dim-witted store keeper would realise something was wrong if the shop suddenly filled with people clamouring for the same stock item).

David

[Also noted by Russell Middleton. PGN]

⚡ Smile for the US Secret Service

Monty Solomon <monty@roscom.com>

Tue, 7 Sep 1999 23:31:47 -0400

Smile for the US Secret Service

by Declan McCullagh, Wired News, 7 Sep 1999

A New Hampshire company began planning in 1997 to create a national identity database for the federal government, newly disclosed documents show. Image Data's US\$1.5 million contract with the US Secret Service to begin digitizing existing driver's license and other personal data was widely reported early this year. But documents unearthed by the Electronic Privacy Information Center reveal the details and scope of the project. See <http://www.wired.com/news/news/politics/story/21607.html>

⚡ NOAA predicts early winter

<seurer@us.ibm.com>

Tue, 7 Sep 1999 09:42:21 -0500

As I ate breakfast this morning I listened to the weather report on the local NOAA weather radio station. As I watched hummingbirds feed from our nectar feeders and squirrels scamper around the yard I was quite surprised to hear that the temperature was 61 degrees F and the wind chill was 64 degrees below zero. Time to break out the parkas!

Sometime last year NOAA began to broadcast forecasts, current conditions reports, and other relatively "fixed" information via a computer generated voice system. Either someone entered bad data or whatever computes the wind chill was broken this morning. A person reading the current conditions would probably have caught the error and certainly would not have kept repeating the bad data.

Bill Seurer, Bill_Seurer@us.ibm.com, Compiler Development, IBM, Rochester, MN
<http://w3.rchland.ibm.com/~seurer/> <http://www.seurer.net>
Bill@seurer.net

✶ The real story on Centaur/Milstar ([RISKS 20.36](#), 20.39, 20.49)

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>
Tue, 03 Aug 1999 11:54:50 +0200

Aviation Week points out on 26 Jul 1999 (p27) that the Centaur upper-stage failure was in fact caused by a programming error. Someone entered a roll-rate filter constant at one-tenth of its proper value (-0.1992476 rather than -1.992476). Not only that, but the USAF investigation determined that "officials overlooked information present during the launch process that a software flaw existed".

Whether or not evidence was present during the launch process, how come such an error wasn't caught during debugging, inspection, component bench test, integration test, and all those other things software and system

developers
are supposed to do?

[To my knowledge, this is only the second verified and public example of a simple programming error (equivalent to a typo) that I know of in aerospace. The first one was Mariner, and as far as I know that's the only one in the RISKS archives. There has been some discussion on certain mailing lists about examples of simple programming errors in critical systems. PBL]

Prof. Peter Ladkin Ph.D. <http://www.rvs.uni-bielefeld.de>
University of Bielefeld, Germany Mobile: +49 (0)171 755 8838

🦆 If it quacks on 1/1/2000, it must be a Y2K duck

Win Treese <treese@openmarket.com>
Tue, 07 Sep 1999 00:14:29 -0400

I received a notice recently that one of Verisign's root keys expires at the end of 1999, and users of Netscape browsers (version 4.05 and earlier) need to get an updated certificate to avoid warnings about expired keys.

This in itself isn't a big problem--we expect certificates to expire, although it can be rather inconvenient. The problem comes from the timing:
anyone seeing odd behavior (such as an extra dialog box) on or near 1/1/2000 is likely to blame it on a Y2K problem, whether that's appropriate or not.

Apparently this fact has not been lost on Verisign's competitors, at least

according to Verisign's FAQ on the matter, at:

<http://www.verisign.com/server/cus/rootcert/facts.html>

Moral of the story: schedule software dates when nothing else important is known to be happening.

Win Treese, Open Market, Inc. treese@openmarket.com

🔥 Food expiry date misreading risks

Dr John Stockton <jrs@merlyn.demon.co.uk>

Fri, 10 Sep 1999 07:48:50 +0100

[This topic is raised in news:uk.tech.y2k.]

There is a little more in my Web page

<URL: <http://www.merlyn.demon.co.uk/date2k-3.htm#Food>>.

Subject : Y2K - User Misinterpretation of Food Expiry Dates

Confusion between two digits meaning Year 20## and meaning Year 19## is well understood; misidentification of ## fields in dates between Y, M, D has been discussed in Y2K newsgroups; the food trade will understand the date formats on their products.

However, one problem is perhaps not well-realised : the use of ## fields in expiry dates on the packaging of foods, together with the circumstances of domestic food storage, leads to the probability that many of those who finally use these packaged foods may misunderstand the dating formats.

For example, an item sold in March 2000 may be marked for use by "OCT 01" - does it have a six- or an eighteen- month life? If it is discovered in the back of the cupboard on 2000-09-20, should it be eaten soon, or is there a safe year left? Many errors can be expected.

Remember that some food travels, some amateur cooks travel, date formats vary, ...

If the famed cook, Great-Aunt Philomena o'Kerry, on her first trip ever out of Erin, visits the kitchen of her Great-Niece in Troy, AL, USA, will she be safe?

John Stockton, Surrey, UK. jrs@merlyn.demon.co.uk
<URL: <http://www.merlyn.demon.co.uk/>>

🔥 Army dumps NT, moves to Mac

Martin Minow <minow@pobox.com>
Fri, 10 Sep 1999 08:38:15 -0700

<<http://slashdot.org/article.pl?sid=99/09/10/1034202&mode=flat>>
Slashdot reports that the Army got bit once too often by script kiddies and moved their web servers to Macs running WebStar. The Army press-release is at: <<http://www.dtic.mil/armylink/news/Sep1999/a19990901hacker.html>>

Martin Minow, minow@pobox.com

[See also Army Bombs NT, Buys Mac, by James Glave, 13 Sep 1999, <http://www.wired.com/news/news/politics/story/21725.html>, which notes that, subsequent to a wave of breakins to their

Website,

the Army is now using a WebSTAR server and an Apple computer for the

Army's homepage. Diversity is of course highly desirable in attempting

to attain security. Having nothing but a single system that is flawed

is clearly a bad idea. Having different systems that are flawed is also

a bad idea, so ultimately we need some meaningfully secure servers! PGN]

⚡ New Hotmail breach reported

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

Wed, 15 Sep 1999 13:09:12 -0500

Another -- albeit potentially less serious -- flaw has emerged in Microsoft's Hotmail service. This one displays a bogus login screen, and

captures the password. The flaw was found by Georgi Guninski, a Bulgarian

security consultant. All it takes is a little JavaScript in an HTML "STYLE"

tag in an e-mail message. The flaw appears to have many other nasty uses as

well. According to Guninski, "This is not a browser problem, it is

Hotmail's problem." [Source: CNN, 14 Sep 1999; PGN-ed]

⚡ New ICQ Trojan (CJNN51)

"Patrick O'Beirne" <pobeirne@sysmod.ie>

Mon, 13 Sep 1999 05:43:12 +0100

>From: CJNN <CJNN@unity.linmedia.co.jp>

>Subject: CJNN51 -- Japan e-biz news
>Date: Mon, 13 Sep 1999 11:25:52 +0900
>
>* * * * C O M P U T I N G J A P A N --- N E W S N E T * * * *
>A weekly roundup of news and information from Computing Japan
> (<http://www.cjnn.com>)
>
>SIGN UP: Send e-mail to: join-cjnn@unity.linmedia.co.jp
> (no subject or body text is needed)
>LETTERS: Send e-mail to: editor@cjnn.cjmag.co.jp
> (use also for making inquiries)
> [...]
>+++ BUG WATCH
>
>-> New ICQ Trojan
>
>A new Trojan horse circulating the Internet disguised as a
>JPEG image is stealing ICQ passwords from users hard drives
>and take control of the ICQ accounts. There are more than
>42m ICQ accounts, but apparently only those with early-
>registered shorter ID lengths are vulnerable. If this has
>happened to you, you can get your registration
>re-authenticated at ICQ.com. (Source: CJNN extract from
>CNET, news.com, Sep 9, 1999)
>
><http://news.cnet.com/news/0-1005-200-114889.html?tag=st>
>
>-> Backup Exec fix
>
>Running Seagate's Backup Exec program may cause errors on
>Microsoft Windows 95, giving the error message: "Bewin32
>reported the start catalog failed - unknown error 0x1."
>
>You can fix the problem by deleting the catalog files.
> 1) Close Backup Exec.
> 2) Open Windows Explorer.
> 3) Browse to [path]\Seagate\Backup Exec\system\catalogs
> directory.
> 4) Delete all the files in that directory.
> 5) Attempt to open Backup Exec.
>
>(Source: CJNN extract from BugNet, Sep 8, 1999)
><http://www.msnbc.com/news/309570.asp>

Patrick O'Beirne B.Sc. M.A. FICS. Systems Modelling Ltd, Tara Hill, Gorey, Co. Wexford, IRELAND <http://www.sysmod.com> +353 (0)55 22294

✦ Macro viruses and Word'97's built-in macro detector/disabler

Gisle Hannemyr <lunchbreak@hannemyr.com>

15 Sep 1999 13:08:29 +0200

Some recent virus profiles has described Word macro viruses that -- it is claimed -- will turn off the macro warning/disabling feature of Word 97.

For example, see the following descriptions of W97M/Cont.A:

<http://vil.nai.com/vil/vm10259.asp>

<http://www.Datafellows.com/v-descs/cont.htm>

http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=W97M_CONT.A

and the following, of a (different?) strand called W97M/Thus.A:

http://www.norman.no/corporate/documents/w97m_thus.htm

If these alerts say what I believe they say, there is great cause for concern.

IMHO. virus protection software can not be relied on as the only measure to prevent macro virus activation. There is a number of reasons for this, but the main reason is that there always elapses some time between emergence of a new computer virus and when new virus signature files covering the new virus becomes available to end users such as myself.

Therefore, I have always relied on the built-in macro warning/
disabling
feature of Word'97 as additional protection. If an (unknown)
document is
reported by Word to contain macros when opened, I use this built-
in feature
to disable all macros before proceeding. So far, I have
believed that this
practice has provided me with full protection against macro
virus infection.

If this built-in detection can be circumvented or disabled, then
this belief
is clearly false. Instead, it seems that opening Word documents
created by
third parties should be avoided, and one should instead inform
all parties
one exchange documents with that one will only accept documents
in a
macro-less format (such as plain text or RTF).

While this may be the sensible approach anyway, it will be a
huge task (at
least in my environment) to convince all my colleagues and
collaborators
that they should stop using Word's .doc format as a document
interchange
format.

Therefore:

- How paranoid should I be :-) ?
- How technically feasible is it for a macro virus to disable the
built-in macro detector?
- Has the claim about Word'97's built-in macro detection/
disabling
being flawed in this way been confirmed by other sources than
by
the specific companies(*) that are my sources.

(*)They are all fine companies, but they are also in the
business of
selling virus protection and therefore they also have a clear

interest

in making the public distrust Word'97's built-in measures against the macro virus problem.)

- gisle hannemyr (gisle@hannemyr.no - <http://home.sol.no/home/gisle/>)

🔥 Microsoft Installs US Spy Agency with Windows

<main@radsoft.net>

Wed, 08 Sep 1999 22:20:59 +0000

Research Triangle Park, NC - 31 August 1999 - Between Hotmail hacks and browser bugs, Microsoft has a dismal track record in computer security.

Most of us accept these minor security flaws and go on with life. But how is an IT manager to feel when they learn that in every copy of Windows sold, Microsoft may have installed a 'back door' for the National Security Agency (NSA - the USA's spy agency) making it orders of magnitude easier for the US government to access their computers?

While investigating the security subsystems of WindowsNT4, Cryptonym's Chief Scientist Andrew Fernandes discovered exactly that - a back door for the NSA in every copy of Win95/98/NT4 and Windows2000. Building on the work of Nicko van Someren (NCipher), and Adi Shamir (the 'S' in 'RSA'), Andrew was investigating Microsoft's CryptoAPI architecture for security flaws. Since the CryptoAPI is the fundamental building block of cryptographic security in

Windows, any flaw in it would open Windows to electronic attack.

Normally, Windows components are stripped of identifying information. If the computer is calculating

```
number_of_hours = 24 * number_of_days
```

, the only thing a human can understand is that the computer is multiplying $a = 24 * b$. Without the symbols "number_of_hours" and "number_of_days", we may have no idea what 'a' and 'b' stand for, or even that they calculate units of time.

In the CryptoAPI system, it was well known that Windows used special numbers called cryptographic public keys to verify the integrity of a CryptoAPI component before using that component's services. In other words, programmers already knew that windows performed the calculation

```
component_validity = crypto_verify(23479237498234..., crypto_component)
```

, but no-one knew exactly what the cryptographic key "23479237498234..." meant semantically.

Then came WindowsNT4's Service Pack 5. In this service release of software from Microsoft, the company crucially forgot to remove the symbolic information identifying the security components. It turns out that there are really two keys used by Windows; the first belongs to Microsoft, and it allows them to securely load CryptoAPI services; the second belongs to the NSA. That means that the NSA can also securely load CryptoAPI services... on your machine, and without your authorization.

The result is that it is tremendously easier for the NSA to load unauthorized security services on all copies of Microsoft Windows, and once

these security services are loaded, they can effectively compromise your entire operating system. For non-American IT managers relying on WinNT to operate highly secure data centers, this find is worrying. The US government is currently making it as difficult as possible for "strong" crypto to be used outside of the US; that they have also installed a cryptographic back-door in the world's most abundant operating system should send a strong message to foreign IT managers.

There is good news among the bad, however. It turns out that there is a flaw in the way the "crypto_verify" function is implemented. Because of the way the crypto verification occurs, users can easily eliminate or replace the NSA key from the operating system without modifying any of Microsoft's original components. Since the NSA key is easily replaced, it means that non-US companies are free to install "strong" crypto services into Windows, without Microsoft's or the NSA's approval. Thus the NSA has effectively removed export control of "strong" crypto from Windows. A demonstration program that replaces the NSA key can be found on Cryptonym's website.

Cryptonym: Bringing you the Next Generation of Internet Security, using cryptography, risk management, and public key infrastructure.

Interview Contact:

Andrew Fernandes <andrew@cryptonym.com>

Telephone: +1 919 469 4714 Fax: +1 919 469 8708

Cryptonym Corporation, 1695 Lincolnshire Boulevard, Mississauga, Ontario

Canada L5E 2T2 <http://www.cryptonym.com>

⚡ Commentary on Back Orifice

Bruce Schneier <schneier@counterpane.com>

Thu, 26 Aug 1999 16:39:12 -0500

Back Orifice 2000 [1]

Back Orifice is a free remote administration tool for Microsoft Windows.

It's also one of the coolest hacking tools ever developed.

Originally

released last July, Back Orifice 2000 (BO2K) is the current release of the

software. It works on Windows 95, Windows 98, and Windows NT.

It is much

better written than the original Back Orifice. And it's free, and open source.

There are two parts: a client and a server. The server is installed on the

target machine. The client, residing on another machine anywhere on the

Internet, can now take control of the server.

This is actually a legitimate requirement. Perfectly respectable programs,

like pcAnywhere or Microsoft's own Systems Management Server (SMS), do the

same thing. They allow a network administrator to remotely troubleshoot a

computer. They allow a remote tech support person to diagnose problems.

They are mandatory in many corporate computing environments.

Remote administration tools also have a dark side. If the server is

installed on a computer without the knowledge or consent of its owner, the

client can effectively "own" the victim's PC.

Back Orifice's difference is primarily marketing spin. Since it is not distributed by a respectable company, it cannot be trusted. Since it was written by hackers, it is evil. Since its malicious uses are talked about more, its benevolent uses are ignored. That's wrong; pcAnywhere is just as much an evil hacking tool as Back Orifice.

Well, not exactly. Back Orifice was designed by a bunch of hackers with fun in mind. Not only can the client perform normal administration functions on the server's computer -- upload and download files, delete files, run programs, change configurations, take control of the keyboard and mouse, see whatever is on the server's screen -- but it can also do more subversive things: reboot the computer, display arbitrary dialog boxes, turn the microphone or camera on and off, capture keystrokes (and passwords). And there is an extensible plug-in language for others to write modules. (I'm waiting for someone to write a module that automatically sniffs for, and records, PGP private keys.)

Back Orifice is also designed to hide itself from the server's owner. Unless the server's owner is knowledgeable (and suspicious), he will never know that Back Orifice is running on his computer. (Other remote administration tools, even SMS, also have stealth modes; Back Orifice is just better at it.) Anti-virus software has been updated to detect default Back Orifice configurations, but that will only solve most of the problem. Because Back Orifice is configurable, because it can be downloaded in

source form and then recompiled to look different...I doubt that all variants will ever be discovered.

Okay, so who's to blame here? The Cult of the Dead Cow wrote and released Back Orifice. Surely the world is not a safer place because, as CDC's Sir Dystic put it: "every 14-year-old who wants to be a hacker will try it." BO2K's slogan is "show some control," and many will take that imperative seriously. Back Orifice will be used by lots of unethical people to do all sorts of unethical things. And that's not good.

On the other hand, Back Orifice can't do anything until the server portion is installed on some victim's computer. This means that the victim has to commit a security faux pas before anything else can happen. Not that this is very hard: lots of people network their computers to the Internet without adequate protection. An attacker can even ask the victim to install Back Orifice (social engineering might help); the Worm. ExploreZip worm of this spring did exactly that. Still, if the victim is sufficiently vigilant, he can never be attacked by Back Orifice.

But what about Microsoft's computing environment? One of the reasons Back Orifice is so nasty is that Microsoft doesn't design its operating systems to be secure. It never has. Any program that runs in Microsoft Windows 95 and 98 can do anything. In Unix, an attacker would first have to get root privileges. Not in Windows. There's no such thing as limited privileges, or administrator privileges, or root privileges. Microsoft

assumes that anyone who can run a program can reformat the hard drive. This might have made some sense in the age of isolated desktop computers; after all, if you could run a program, you were standing in front of the machine. But on the Internet, this is absurd.

Windows NT was designed as a secure operating system, more or less. There are provisions to make Windows NT a very secure operating system, such as privilege levels in separate user accounts, file permissions, and kernel object access control lists. However, the configuration that makes Windows NT secure is very very far and distant from the default installed configuration. Microsoft admits this. You have to make 300+ security checks and modifications to Windows NT to make it secure in its default configuration [2]. And on top of this, Microsoft assumes that most users have Administrator access to their desktop machines anyway. They only really worry about network security, not host-end security, which is where they are seriously vulnerable to attacks like Back Orifice 2000. Windows NT could be secure, but Microsoft refuses to ship the OS in that condition (presumably they worry that their spiffy animated fading menu bars may be overlooked).

Malicious remote administration tools are a major security risk. What Back Orifice has done is made mainstream computer users aware of the danger. Maybe the world would have been safer had they not demonstrated the danger so graphically, but I am not sure. There are certainly other

similar tools
in the hacker world -- one, called BackDoor-G, has recently been
discovered
-- some developed with much more sinister purposes in mind. And
Microsoft
only responds to security threats if they are demonstrated.
Explain the
threat in an academic paper and Microsoft denies it; release a
hacking tool
like Back Orifice, and suddenly they take the vulnerability
seriously.

Back Orifice Home Page:

<http://www.bo2k.com/>

Commentary:

<http://www.zdnet.com/zdnn/stories/news/0,4586,2127049,00.html>

<http://www.infoworld.com/cgi-bin/displayArchive.pl?/99/30/o03-30.36.htm>

Microsoft's Systems Management Server:

<http://www.microsoft.com/smsgmt/techdetails/remote.asp>

<http://www.cultdeadcow.com/news/pr19990719.html>

BackDoor-G:

<http://www.zdnet.com/zdnn/stories/news/0,4586,2267379,00.html>

[1] This essay originally appeared in Crypto-Gram, my monthly
newsletter
on computer security and cryptography. You can subscribe or
read back
issues at <http://www.counterpane.com/crypto-gram.html>.

[2] Since writing this, I have been asked about the 300+
figure. I heard it
second hand, so I queried the Usenet newsgroup
comp.os.ms-windows.nt.admin.security asking if it was folklore
or truth.
The consensus seemed to be that the number was somewhere between
50 and
3000, and 300 wasn't an unreasonable estimate. A good checklist
is

available at <http://people.hp.se/stnor/>.

⚡ CPSR Conference: The Internet Gold Rush of '99

<sevoy@quark.cpsr.org>

15 Sep 1999 01:48:31 -0000

Now you can register online at

<https://swww.igc.apc.org/cpsr/registrationForm99.html>.

Early Registration rates end Friday, September 17th.

Computer Professionals for Social Responsibility annual conference

THE INTERNET GOLD RUSH OF '99:

CAN WE PAN FOR GOLD WHILE SERVING THE GOOD?

THE PURSUIT OF WEALTH AND EQUITY IN CYBERSPACE

2-3 October 1999 (9:00 am to 5:30 pm)

Building 420 (Jordan Hall), Room 40, Stanford University,
Stanford, CA

NORBERT WIENER AWARD RECEPTION honoring THE OPEN SOURCE/FREE SOFTWARE MOVEMENT

2 October 1999 (6:00 - 8:00 pm)

AT&T Patio (outside of Gates Hall), Stanford University,
Stanford, CA

FEATURED SPEAKERS include Gray Brechin (Keynote talk on Historical Amnesia

in the Silicon Gold Rush) Eric Raymond, Larry Wall, Brian Behlendorf, Craig

Newmark, Cem Kaner, Barbara Simons, Peter Neumann, Madeline Stanionis, Seth

Fearey, Ben Politzer, Eric Sklar, Pavel Curtis, Scott Hassan, Laura Breedan.

Saturday sessions include

* SOCIAL RESPONSIBILITY AND FINANCIAL SUCCESS - OXYMORON?

* THE DIGITAL DIVIDE: IS THE INTERNET AS GREAT EQUALIZER LOSING

GROUND?

* SOFTWARE AT THE CROSSROADS: OPEN-SOURCE SOFTWARE AND THE
UNIFORM COMPUTER
INFORMATION TRANSACTIONS ACT (UCITA)

CPSR's prestigious Norbert Wiener Award for Social
Responsibility in
Computing Technology is being awarded to the Open Source/Free
Software
Movement. This movement profoundly challenges the belief that
market mechanisms are always best-suited for unleashing
technological innovation. This voluntary and collaborative
model for
software development is providing a true alternative to
proprietary,
closed software.

CPSR ANNUAL MEETING, SUNDAY, 3 OCTOBER 1999, 9:30am - 2:30pm
Building 420 (Jordan Hall), Room 40, Stanford University,
Stanford, CA

Conference Committee Karen Coyle, Paul Czyzewski, Jeff Johnson,
Coralee Whitcomb, Susan Evoy

Complete information at [HTTP://WWW.CPSR.ORG/](http://www.cpsr.org/),
registration via [https://swww.igc.apc.org/cpsr/
registrationForm99.html](https://swww.igc.apc.org/cpsr/registrationForm99.html)

Susan Evoy, Deputy Director <evoy@cpsr.org> <[http://www.cpsr.
org/home.html](http://www.cpsr.org/home.html)>

Computer Professionals for Social Responsibility, P.O. Box 717,
Palo Alto
CA 94302, Phone: (650) 322-3778, Fax: (650) 322-4748



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 58

Friday 17 September 1999

Contents

- [The Microsoft/NSA Crypto Brouhaha](#)
[Dan Wallach](#)
- [Hurricane Floyd stops trains in Michigan](#)
[Ed Ravin](#)
- [USA Today weather page - no reasonability check](#)
[Bob Dainauski](#)
- [Date failure on weather.com](#)
[Eric Remy](#)
- [Emergency Alert System interrupts Hurricane Announcement, and crashes](#)
[Withheld](#)
- [Hacker attack on NASDAQ, AMEX, and others](#)
[Keith A Rhodes](#)
- [Hacker admits attacks on NATO, USIA Web pages](#)
[Doneel Edelson](#)
- [Indonesian Year 2000 plans](#)
[Fraser McHarg](#)
- [Yet another date-related problem](#)
[Geoff Kuenning](#)
- [Smart Dust](#)
[Steve Holzworth](#)

- [Re: The real story on Centaur/Milstar](#)
[Rick Carter](#)
- [Terrorist bombing botched due to timing error...](#)
[Joan L. Grove Brewer](#)
- [NSI blows it again---is there no lower bound to their idiocy?](#)
[Lenny Foner](#)
- [HTML on Win Desktop](#)
[Robert Graham](#)
- [E-commerce stupidity](#)
[Michael Taylor](#)
- [Re: Refrigerator gasket frozen out](#)
[Henry Spencer](#)
- [Risks of old RISKS](#)
[Ochran Industries](#)
- [Info on RISKS \(comp.risks\)](#)

✂ [The Microsoft/NSA Crypto Brouhaha \(Re: Fernandes, RISKS-19.57\)](#)

Dan Wallach <dwallach@cs.rice.edu>

Thu, 16 Sep 1999 22:57:14 -0500

Andrew Fernandes of Cryptonym has publicized an interesting feature of Microsoft's Crypto Service Provider (CSP) architecture [1]. Microsoft's design goal appears to have been preventing "unauthorized" people from writing their own CSP modules and dropping them into Windows (and thus circumventing US crypto export policy). Microsoft's architecture does this by verifying a digital signature on the crypto module before loading it.

Microsoft included an additional public key, allegedly belonging to the NSA.

One might imagine that the NSA, which most likely has homegrown cryptography it prefers to use, might want to distribute its own CSP to its clients without the intervention of Microsoft. Microsoft has said in public that this is a "backup" key, which is also believable.

My complaint with Fernandes' analysis is his implication that this might allow for NSA espionage or some other nefarious activity. As I understand it, Microsoft's architecture has no provision for some third party throwing a new CSP module at a target host and forcing it to be installed (whether signed by the NSA or not). If someone truly wished to perform some kind of espionage, they would need some other way of breaking into the target machine, and would be more likely to install a "remote administration service" like Back Orifice than to change out the crypto module.

Needless to say, Fernandes' message has caused a wide range of conspiracy theorists to come out of the woodwork (for example, check out the Slashdot discussion threads [2]). Fernandes will claim that this feature still "makes it easier" for the NSA to somehow attack you. This appears to be completely wrong. Indeed, this feature seems to make it much easier for parties outside the US to enhance the cryptographic strength of their system and thus make it harder for the NSA or anyone else to attack them.

In the past two weeks, this has been discussed ad nauseum in a number of technical forums. The Telcom Digest has some excellent summaries of what

happened and how Microsoft's CSP architecture works [3]. NTBugTraq has a nice article [4], and Bruce Schneier has a concise article on his page [5].

What are the RISKS and morals of the story?

- Elaborate cryptographic architectures designed to obey the US export

crypto standards may have bugs in them. It's somehow ironic that a bug in

Microsoft's CSP architecture effectively allows anyone to install their own

CSP module, without the permission of anyone.

- Security through obscurity still doesn't work. People will expend amazing energies to reverse engineer code to get around any restrictions it may have.

- Going public with a story that sounds tasty to conspiracy theorists will

get you a lot of press ("Microsoft in bed with NSA, film at 11!"), whether

or not your arguments are technically sound. Security researchers thus have

a responsibility to verify their claims.

And, perhaps most ironic of all, the Clinton administration has now

announced it is relaxing US crypto export restrictions [6], allowing

companies like Microsoft to effectively export anything they want, and thus

rendering the whole CSP architecture an anachronism. The new policy doesn't

make crypto completely free of regulation (and Microsoft may yet need to

keep its CSP architecture around), but that's a topic for another RISKS

posting.

Dan Wallach, Rice University

[1]<http://www.cryptonym.com/hottopics/msft-nsa.html>

[2]<http://slashdot.org/article.pl?sid=99/09/03/0940241&mode=thread>

(also) <http://slashdot.org/article.pl?sid=99/09/09/138209&mode=thread>

[3]http://hyperarchive.lcs.mit.edu/telecom-archives/archives/back.issues/recent.single.issues/V19_%23379

[4]<http://ntbugtraq.ntadvice.com/default.asp?sid=1&pid=47&aid=52>

[5]<http://www.counterpane.com/nsakey.html>

[6]<http://www.wired.com/news/news/politics/story/21786.html>

[Incidentally, I ran the Fernandes item in [RISKS-20.57](#) fully aware that

Dan's subsequent discussion was needed to complete the story, but wanted

to provide the sequential nature of its unfolding. PGN]

🌀 Hurricane Floyd stops trains in Michigan

<eravin@panix.com>

Tue, 14 Sep 1999 21:00:55 -0400 (EDT)

The US passenger rail company, Amtrak, has announced service changes due to

Hurricane Floyd - as one might suspect, they are canceling trains to and

from Miami and North Carolina, but some of the changes reach much farther

than any of the hurricane's weather effects.

According to Amtrak's Web site, because some Amtrak trains are

dispatched
from the CSX (US freight rail) operations center in
Jacksonville, Florida (a
location where they fear the seas will rise 20 feet due to the
hurricane),
they are canceling trains between Chicago and Grand Rapids,
Michigan, as
well as several other trains to and from Chicago.

The Amtrak notice is at <http://www.amtrak.com/news/pr/floyd.html>

[RISKS-8.70](#) mentions CSX's Jacksonville computer-assisted
dispatch operation,
and how it consolidated 34 dispatch offices into one big room.

[Sara Thigpen noted that the shutdown of commuter rail service
in
the Maryland/Washington D.C. area caused massive automobile
commuter
traffic problems, well ahead of the hurricane effects.

Richard Heritage wondered whether CSX has any capability for
decentralized
operation. (Apparently not.) and also wonders what would
have happened
had the hurricane actually knocked out the Florida dispatching
center.

It has been duly noted by various folks that this centralized
control
problem might suggest a serious Y2K risk. We are of course
assured
that "everything is under control." <pun intended by PGN>

Incidentally, I am teaching a course on survivable systems and
networks
in the Engineering Department at the University of Maryland
this fall
(see my Web site). In that context, survivability implies
tolerance to
arbitrary adversities. Last week's lecture took place in a
lightning
storm that knocked out the PC controlling some of the remote

feeds. The

third lecture on 16 Sep was cancelled because of the hurricane. Nothing

like self-referential examples to the problem under discussion... PGN]

⚡ USA Today weather page - no reasonability check

<radainauski@papl.com>

Thu, 16 Sep 1999 09:05:36 -0400

With Hurricane Floyd expected to pass through here (Allentown, PA) today, I thought I'd check the USA Today weather page for an update. The forecast for is for a record high:

THURSDAY: Rain is likely. The high temperature will be 577 degrees

Fahrenheit (303 degrees Celsius).

I saved an image of the page, which was quickly fixed. In this instance the error is more humorous than RISKy, but it serves as another example of a lack of defensive design. A deficiency which could have significantly more serious consequences in other scenarios.

Bob Dainauski - robertd@fast.net

⚡ Date failure on weather.com

Eric Remy <edremy@chemserver.chem.vt.edu>

Thu, 16 Sep 1999 17:55:20 -0400

Like many others, I use weather.com to get daily weather reports. Today I went to get my "Detailed local forecast" and noted that while the forecast seemed accurate so far as I could tell by looking out the window, the date on the forecast read April 28. (It's currently September 16) So is the date wrong or am I seeing the forecast for April 28?

The RISK? Normally, this wouldn't be a big deal, save that as of yesterday, I didn't know if Hurricane Floyd was going to run over my area. I'm on the fringe of the possible storm track and in the mountains, so I'm not following it closely on TV. As more people being getting news and weather reports via the net, Web sites that provide information like this had better be very careful to avoid lawsuits.

Eric D. Remy Chemistry Learning Center Director, Virginia Tech
edremy@chemserver.chem.vt.edu (540)-231-9016

⚡ Emergency Alert System interrupts Hurricane Announcement, and crashes

<[identity withheld by request]>

Fri, 17 Sep 1999

On Monday Sept 13th at 5PM the local news stations here in West Palm Beach, Florida were reading the latest advisory from the National Hurricane Center regarding Hurricane Floyd (winds 155mph) when the Emergency Alert System activated and seconds later crashed leaving nothing but a Blue

Screen on all channels of my Comcast Cable TV System. This Blue Screen persisted for 20 minutes or more and prevented reception of the local news which was announcing a Hurricane Warning (upgraded from a Hurricane Watch) for the local area. What is worse is that the exact same thing happened just one week prior (that time it was for a severe thunderstorm warning and lasted for a full 60 minutes). Comcast doesn't seem to have taken any action other than resetting whatever equipment had malfunctioned, no attempt to learn from this and prevent it from recurring. The recent outage was widespread enough for the local news anchor to mention it and clarify that the outage was not the fault of the TV Station but rather a problem with an unnamed Cable TV system.

The new Emergency Alert System (EAS) is supposed to be an improvement over the Emergency Broadcast System (EBS) but in this case seems to be a step backwards in terms of reliability.

🔥 Hacker attack on NASDAQ, AMEX, and others

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

Thu, 16 Sep 1999 09:49:58 -0500

ZDNN (<http://www.zdnet.com/zdnn/>) reported on 16 Sep 1999 that a group calling themselves United Loan Gunmen had altered Nasdaq and American Stock Exchange Web sites, and claimed responsibility for earlier

attacks on
C-Span, ABC, and Matt Drudge sites. *The New York Times* (in an
AP item,
<http://www.nytimes.com/aponline/w/AP-Nasdaq-Hacked.html>) noted
that ``The
hackers left a taunting message -- the high-tech equivalent of
spray-painting graffiti -- and also claimed to have briefly
created for
itself an e-mail account on Nasdaq's computer.'' [PGN-ed]

⚡ Hacker admits attacks on NATO, USIA Web pages

"Edelson, Doneel" <doneeledelson@aciins.com>

Wed, 8 Sep 1999 08:56:18 -0400

``Zyklon'' (Eric Burns, 19) has pleaded guilty to Web site
attacks on NATO,
Al Gore, and the USIA, and faces up to 5 years, a \$250K fine, and
restitution. His Web Bandit program identifies vulnerable
sites. [Source:
Reuters, 7 Sep 1999, seen on Yahoo! News; PGN-ed]

⚡ Indonesian Year 2000 plans

<Fraser_McHarg@nag.national.com.au>

Mon, 13 Sep 1999 11:18:55 +1000

I admit that I haven't been able to verify this report, but if
only half true
the risks are obvious...

PLN, Indonesia's national electricity board, was recently asked
by an
Indonesian newspaper about its Y2K Preparedness.

The reply is a gem:

"We can observe what happens (at midnight 1999) in Western Samoa, New Zealand and Australia and still have 6 hours to make plans."

Cheers,

Fraser McHarg from the East coast of Australia and contrary to the above report we have two hours to make plans after observing New Zealand :-)

Well, the RISKS archives include cases of systems such as ATMs failing in

New Zealand and the fix being effected before midnight in England.

HOWEVER, the complexity of fixing dynamically detected Y2K bugs may be

different from some of the previous clock problems. PGN]

⚡ Yet another date-related problem

Geoff Kuenning <geoff@cs.hmc.edu>

Mon, 13 Sep 1999 23:52:30 -0700

I was working on a new script last night, and stopped to consider how many output columns would be occupied by a Unix timestamp in the semi-standard decimal representation. Nine digits, right? Always has been, always will be... NOT!

The Unix timestamp first hit 9 decimal digits on March 3, 1973, and it has been inexorably incrementing ever since. A quick check with my time conversion program tells me that at precisely 01:46:40 UTC on Sunday, September 9, 2001, it will need that 10th digit.

This is a much smaller problem than most other date bugs, of course. But I have to suspect that there are a few programs out there that will break, at least to the extent of causing an 80-character output line to wrap to 81.

Geoff Kuenning geoff@cs.hmc.edu <http://fmg-www.cs.ucla.edu/geoff/>

🔥 Smart Dust

Steve Holzworth <sch@unx.sas.com>
Wed, 8 Sep 1999 15:05:48 -0400

From *New Scientist*:

"CLEANLINESS FREAKS have a new rationale for their pathological hatred of dust--it could soon be spying on them.

Packed full of sensors, lasers and communications transceivers, particles of "smart dust" are being designed to communicate with one another. They could be used for a range of applications from weather monitoring to spying. "

See <http://www.newscientist.com/ns/19990828/newsstory2.html>

Steve Holzworth <sch@unx.sas.com> Senior Systems Developer
SAS Institute - Open Systems R&D VMS/MAC/UNIX Cary, N.C.

🔥 Re: The real story on Centaur/Milstar (Ladkin, [RISKS-20.57](#))

Rick Carter <Rick.Carter@umich.edu>

Thu, 16 Sep 1999 13:09:54 -0400 (EDT)

There was a third example that comes to mind here. I clearly remember that, probably in the mid 1980s, a shuttle experiment's data was invalidated because of a mixup in a parameter [...]

Rick Carter, System Administrator, Physics Dept., University of Michigan

Rick.Carter@umich.edu

[I think Rick is referring to the experiment on Discovery (before we began the on-line RISKS, documented in my Risks section of ACM Software Engineering Notes vol 10 no 3, July 1985, and in my Computer-Related Risks book) in which the input "+10,023" for the elevation of a mirror for a laser experiment was interpreted as miles, not feet, resulting in the laser beam being aimed upward (to a point 10,023 miles above sea-level) rather than downward (to a point 10,023 feet above sea-level, at the top of Mona Kea in Hawaii. PGN]

✶ Terrorist bombing botched due to timing error...

"Joan L. Grove Brewer -- Mnemosyne" <pegasus@transport.com>

Sat, 11 Sep 1999 12:52:20 -0700

Last week, Israeli time -- which is not on our western Daylight Savings Time -- fell back. Due to the lack of synchronization between the time in Israel and Palestine, which is on Daylight Savings Time, a car bomb

went off in
Haifa one hour earlier than expected, killing the bomber who was
still in
the car. Israel sets their clocks to coincide with Yom
Kippur... :-)

Did time run out for terrorist bombers?

See Barbara Demick, Knight Ridder Newspapers
[http://www.seattletimes.com/news/nation-world/html98/
alttime_19990911.html](http://www.seattletimes.com/news/nation-world/html98/alttime_19990911.html)

Joan L. Brewer -- A Muse <pegasus@transport.com>
Issaquah, WA 98027 <http://www.transport.com/~pegasus>

⚡ NSI blows it again---is there no lower bound to their idiocy?

Lenny Foner <foner@media.mit.edu>
Thu, 16 Sep 1999 15:27:04 -0400 (EDT)

Network Solutions just spammed (apparently) its entire customer
base with a
message that guarantees we'll see a lot of forged mail
originating from
them. (The message came from integram.org, interestingly
enough, but claims
to be from NSI---thought WHOIS integram.org claims that the
admin and
billing contacts are "no.valid.email@worldnic.net"!))

Parts (a) and (b) of the message said, basically, "you now have
to pay in
advance for a new domain registration" and "we've added you
without warning
to a global directory". (Big deal---that was already available
via NIC
WHOIS, although I haven't checked the directory to see if it's
more
searchable and thus more subject to abuse.) [The message is

P.S. You can call NSI's toll-free number at 888/642-9675. I spent 10 minutes on hold with them, finally got an answer, and said, "Hi there. I just got spam from NSI indicating you'd created an account for me without asking me and I need to you to change the password immediately." They hung up on me after the word "spam". I tried again, was told "only our tech people can do this", was left on hold for 15 minutes, and then was dropped.

P.P.S. Having -finally- gotten through to the URL mentioned in the spam, I've now spent 10+ minutes trying to figure out -how- to actually log in and change my password. Still no luck. Anyone have any clues?

[Also commented on by Marcus Ranum, David Rochberg, Ben Cantrick, Karl Reinsch, Merlyn Kline, T Byfield, and maybe others. PGN]

🔥 HTML on Win Desktop

"Robert Graham" <rob@networkice.com>
Sat, 11 Sep 1999 17:30:03 -0700

HTTP has a feature where it indicates the "Referer", which is the page somebody followed to get to your document. RISKS of this field have been well documented in the past. Here is a new variant.

I peruse my Web server logs occasionally. I found this particular "Referer" item:

file:///D:/WINNT/Profiles/lattimm.000/Desktop/home/idsfaq.html

From this, I know:

1. the user name is "lattimm". Discovering the user name is a frequent first-step in a hacker attack against a machine.

2. On that machine, Windows NT is installed in D:\WINNT. There are many Web-browser attacks that require knowing the exact filename, which is why many people (like me) choose to install in a directory other than c:\winnt or c:\windows.

Solution:

Don't save HTML files to your desktop. Of course, you could always turn off the "Referer" field as well through an add-on product.

Robert Graham, CTO, Network ICE

⚡ E-commerce stupidity

Michael Taylor <mctaylor@arles.ns.ca>

Wed, 8 Sep 1999 17:34:50 -0300 (ADT)

I recently worked on setting up an e-commerce payment system for my business and was surprised with the nonperformance of the "shopping cart" software which I had bought from a local e-commerce "solution provider." While configuring and test the site during my setup I had no problems with it, but after I opened the storefront I had reports that customers were unable to buy anything, not a good thing. It turns out that this "shopping cart" had

violated the URI specs and while older browsers accepted this, the current versions of Communicator and IE did not. This is a simple demonstration of the classic risk of caveat emptor, it also demonstrates how "sloppy" Web design might be acceptable to current versions of the most popular Web browsers, that does not test whether a site is correct (as per HTTP, URI, HTML specifications). Of the professional Web site designers I have contact with, only one occasionally uses a HTML verifier while the rest just check the display of generically configured Communicator and IE browsers.

Since I am involved in e-commerce, a colleague forwarded me a strange e-mail recently. It was a bounce message from the back-end of an order processing system for a large multinational company who had their "orders" mailbox (or related drive) fill up. In original e-mail, and still in the bounced message sent to the customer, was an unencrypted copy of all the order information including all his credit card information. The risks are obvious, an e-mail message which was expect to remain within a "trusted" LAN did not due to a simple and common failure of e-mail delivery. It is not clear how many administrators at the company and his ISP may have also received unencrypted copies of his credit card information.

Michael Taylor mctaylor@arles.ns.ca Arles Trading Company
Linux / BSD software retailer <http://www.arles.ns.ca/>

✶ Re: Refrigerator gasket frozen out (Lee, [RISKS-20.54](#))

Henry Spencer <henry@spsystems.net>

Wed, 15 Sep 1999 16:45:33 -0400 (EDT)

> ... it had to go surface because it was regarded as hazardous cargo.

> I assume that is because it is essentially one big magnet ...

Modern planes generally do still have magnetic compasses, as emergency backups for the more sophisticated hardware.

On the other hand, the classification of magnets as hazardous cargo goes back a long time, to the days of much smaller aircraft and much less sophisticated equipment, when cargo was physically closer to the flight deck and magnetic compasses got more use.

On the third hand :-), that sort of aircraft is still in use in a lot of the world's backwaters, and there is considerable advantage in having uniform hazardous-materials rules, even if that does mean worst-case rules which are a bit stricter than necessary in specific situations.

Henry Spencer <henry@spsystems.net> or <henry@zoo.toronto.edu>

✶ Risks of old RISKS

Ochran Industries <n2585464@sparrow.qut.edu.au>

Fri, 17 Sep 1999 23:03:51 +1000 (EST)

I came across comp.risks, and decided I wanted to read the previous issues, so, starting at volume 1, issue 1, I began reading, using

Lindsay Marshall's wonderful archive (and have noticed that the more the world changes, the risks stay the same!).

I used the gzipped (.gz) version of the original posting, rather than the more flashier Web versions, for various reasons.

Until I came to volume 5. Requesting issue one from the archive page, I got the response: No such issue. Strange. So I tried issue 2, and got the same result. Requested issue 56 - and still got the dreaded "No such issue". So I sent an e-mail off to Lindsay, and waited. And waited and waited. So I thought that he had seen my e-mail, and ignored it. Which turned out to be very, very wrong, on my part.

It turns out that Volume 5 wasn't there due to a disk corruption issue. *But*, Lindsay was on holiday, and thus, could never have read my e-mail. So while I was sitting here, and reading the html versions, and wondering why the problem wasn't getting fixed, Lindsay was totally unaware of the problem.

The Risks

1. Archives get corrupted. They 'loose' files. And you normally don't need to worry, until some stranger comes along and finds that bits are missing, or things are not as they should be. Or worse, *you* need the archives, and find bits missing.

2. Just because you sent that e-mail, don't expect that the person on the other end got it. You may have typed the address wrong (easily

checked). It may have been munched by the maw of the 'net, and gone that place in the universe where all e-mails are finally united with their brethren (I don't know how common this is, but I assume not very). Or, the person on the other end may just not be there. They may be taking a well earned rest from the plagues of e-mail they get every day (which turned out to be true). They may not care, and the request may be one which should never been sent in the first place. And, they may be dead, or missing, and the news just hasn't got to you yet.

So how does this story end? Lindsay returned from his holiday, read my e-mail, and fixed it but good. I came across another missing issue, 12.72, and as soon as it was reported, it was fixed. I'd like to thank you Lindsay, for the wonderful job you have been doing, and PGN for such an excellent job as moderator, guide, and mover. May both your risks ever be insignificant for the rest of all time.

That was a while ago, and had been reading further, when I came across 17.83, in which PGN mention he had fixed a typo. Leaving out the uneasiness which came over me at what amounts to revisionism in my books, the typo had not been fixed in the version I read, as Lindsay archives posts direct from usenet, not from the archive at SRI.

The RISKS:

1. Having multiple, independent archiving sites is great, unless you change

something in one archive, and forget about the others.

2. Changing something in an *archive* copy. As the name suggests, these represent things *as-they-were*, not as-they-should-have-been. There is no need to change things in earlier versions, as a note in the current version ("post x in volume y issue z got 'c' wrong, as it is supposed to be 'd'). Perhaps a pointer to issue z+1 in issue z is okay, as long as it is clear it is an addition, and clearly visible as such, but altering archived versions of *anything* is skating on thin ice.

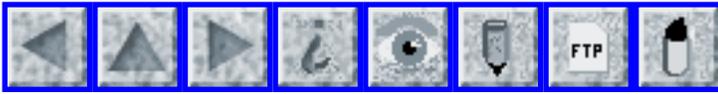
westyX - n2585464@sparrow.qut.edu.au

[Don't forget, Lindsay's Newcastle archive is a beautiful mirror of the much simpler SRI archive at ftp.sri.com (cd risks) that merely gives the raw issues. I certainly believe in redundancy!

On those rare occasions when I make in the SRI archive, I identify the change, and almost always remember to let Lindsay known. I think putting in an occasional N+1 pointer that something will be corrected in the next issue is a very sound practice, because otherwise erroneous stuff tends to propagate without correction.

And I too thank Lindsay repeatedly for the wonderful job he is doing.

I even had a chance to see him in person when I was in Newcastle last week! 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 20: Issue 59

Thurs 23 September 1999

Contents

- [Mars Climate Observer failure](#)
[PGN](#)
- [UK rail disaster inquiry: driver had his feet up!](#)
[Bernard Lyons](#)
- [AT&T nationwide cellphone service goes down, 3000 miles from Floyd](#)
[John Gilmore](#)
- [India and Pakistan in Web war](#)
[Martin Minow](#)
- [Sweet Y2K angle](#)
[Sara Thigpen](#)
- [1 Oct 1999 as a Y2K problem date?](#)
[David Wittenberg](#)
- [Re: The real story on Centaur/Milstar](#)
[Marc Passy](#)
- [Re: Macro viruses and Word'97's built-in macro detector/disabler](#)
[David Chess](#)
- [Massive hole in NSI web-based e-mail](#)
[dotcomnow](#)
- [An easy 'out' for dotcomnow.com accounts](#)
[Art Delano](#)

- [More data on the NSI spam: acct names and how to change passwords](#)
[Lenny Foner](#)
 - [Final bit of info re NSI spam](#)
[Lenny Foner](#)
 - [Re: NSI blows it again](#)
[Brian Clapper](#)
 - [Re: 22nd National Information Systems Security Conference](#)
[Ed Borodkin](#)
 - [15th ACSAC Advance Program](#)
[Vince L. Reed](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Mars Climate Observer failure

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

Thu, 23 Sep 99 13:27:12 PDT

The \$125M Mars Climate Observer probe had seemingly been approaching Mars on target, but somehow managed to get within about 60 km of Mars -- rather than the planned 160 km -- an altitude that was 25 km too close for the probe to survive. This too-close approach is believed to have resulted from erroneous commands sent to the probe, although there are now suspicions that the probe had been off course since the last previous correction on 15 Sep.

[Source: http://www.cnn.com/TECH/space/9909/23/mars_orbiter.04/ , CNN news, 23 Sep 1999]

[Mars has been a tough target. The Soviets lost both Phobos I (faulty remote software upgrade, 1988) and Phobos II (bad antenna realignment), and another mission that was destroyed on launch (1996), after

the earlier

loss of an attempted Mars orbiter in 1971. The U.S. lost a 1993 Observer,

and more recently the Mars Rover Pathfinder ([RISKS-19.49](#) to 56). There

have of course been some successes, with the Viking landers (1970s) and

Pathfinder (1997).]

✈ UK rail disaster inquiry: driver had his feet up!

Bernard Lyons <bernardl@indigo.ie>

Wed, 22 Sep 99 21:28:34 +0000

The driver of the high-speed passenger train that crashed in 1997 killing 7 and injuring 150 had been seen earlier on that trip with both feet up on the dashboard of his cab, leading to speculation that he had weighted down the dead-man's switch. He later drove through two warning signals and a red stop signal before colliding with a freight train crossing the line in front of him at Southall, in West London, en route to Paddington Station in London. The inquiry has now finally begun. The inquiry heard that the train's Automatic Warning System (AWS) -- which sounds a klaxon when the train goes through danger lights -- had been switched off after apparently malfunctioning earlier in the day. The train was also fitted with Automatic Train Protection (ATP), but this was also switched off because the driver who had been in charge of the train earlier in the day was not trained to use it; that system would have automatically prevented the train

from
running the stop signal. Great Western was already fined a
record 1.5M
pounds for a breach of the Health and Safety Act. [Source: BBC
website, 20
Sep 1999 <[http://news.bbc.co.uk/hi/english/uk/
newsid_452000/452732.stm](http://news.bbc.co.uk/hi/english/uk/newsid_452000/452732.stm)>;
PGN-ed]

⚡ AT&T nationwide cellphone service goes down, 3000 miles from Floyd

John Gilmore <gnu@toad.com>
Sat, 18 Sep 1999 21:29:41 -0700

I am an AT&T customer on the Digital One plan, which sells me a
cellphone
that works nationwide with no roaming or long-distance charges.
The problem
is that the system is not robust. If local phone circuits stop
working in
particular places, the AT&T network won't complete calls to
phones whose
number happens to be there, even to cellphones that aren't
anywhere near the
affected area.

My cellphone number is in the 914 318 exchange (New York
[Westchester] metro
area). I am physically located today in San Francisco. I can
make calls,
but nobody can call me. When I make a call to the cellphone
from a San
Francisco land-line that has AT&T long distance service, AT&T
routes my call
through New York, which results in a recording saying that the
hurricane
makes it impossible to complete my call. Why does AT&T route my
call

through New York? Because its long-distance network is too stupid to realize that it's calling an AT&T mobile exchange, and dump the call into a local (California) AT&T mobile switch, which could provide direct routing to wherever the phone actually is.

When I call my cellphone from itself, I still get the recording! The local cellular switch is too stupid to complete outgoing calls to this number locally, even though it knows how to handle incoming calls for this phone number!

There's an efficiency issue about why every call to the cellphone should go to New York and then to the phone's location, but much more important is the robustness issue. What other parts of AT&T's network will take out my cellphone if they go down? Some national switching center in tornado territory in the Midwest? Some billing center under a blizzard in Canada?

I hope that as AT&T redesigns its network for IP-based telephony, it will address some of these issues.

John

PS; One of the other little things AT&T doesn't tell you will break until after you notice it: their voicemail system won't answer your calls if you roam into an analog cellular system! They just ring and ring and ring. I think this is true even if your cellphone is powered off, if the last place it was on was analog.

PPS: I hope somebody else in RISKS is covering why it's been days since San Franciscans can call New York, at least on AT&T circuits. Are any of the other carriers doing any better? I'd try a few, but none of them put their prefix code in their ads in the brand-new Pac Bell phone book!

✶ India and Pakistan in Web war

Martin Minow <minow@pobox.com>

Wed, 22 Sep 1999 09:52:28 -0700

Slashdot <<http://www slashdot.com>> references an article in the Australian web site (affiliated with the Sydney Morning Herald), <<http://www.it.fairfax.com.au/communications/19990921/A12383-1999Sep20.html>>

that describes attacks on the opposing country's websites:

"At the same time [India and Pakistan] have been fighting a war over information, with several Internet resources hacked in both countries. With some of the best software skills in the world, the fighting over the Internet is just as ferocious as in the snow-capped mountains of Kashmir.

"Several top Indian and Pakistani computer professionals in America and Europe are "helping" their respective governments by supplying information on the best way to harm the enemy's computer systems."

Transcribed by Martin Minow, minow@pobox.com ps: what I find most interesting about this is the way in which the Internet makes international news more accessible -- which I see as an anti-Risk.

⚡ Sweet Y2K angle

Sara Thigpen <thigpen@gmpvt.com>

Wed, 22 Sep 1999 13:11:55 -0400

I suppose another Risk of the Y2K hysteria is this "sweet" hoax. I received this from a cousin, who has now been directed to (a) desist from sending me spam and chain letters; and (b) an Urban Legends web site.

>Date: Friday, August 06, 1999 12:15 PM

>Subject: FREE M & M's

>

>Have some fun-this is not a hoax.

>

>Hi. My name is Jeffrey Newieb. I am a marketing analyst for M & M's

>chocolate candies based in Hershey, Pennsylvania.

>

>As the year 2000 approaches, we want to be the candy of the millennium -

>As you may already know, the roman numeral for Y2 is MM. We are

>asking you to pass on this e-mail to 5 friends. Our tracking device is

>calculating how many e-mails you send out. Everytime it reaches 2000

>people, you will receive a free case (100 individual 55 gram packs) of

>delicious M&M candies. That means the more people this reaches, >the more candy you're going to get.

>

>Mmmmmm.. yummy M & Ms the year 2000!!

>

>Remember, nothing but no M & M's will come your way if you do not

>share this with at least 5 people

>
>Don Fry, CPC, President
>Dunhill of Corpus Christi, Inc.
>Voice: (361) 225-2580
>Fax: (361) 225-3888

Anyone want to call him? I didn't.

And when I told my cousin there's no such thing as a "tracking device", I got this reply:

>What do ya mean, they don't have the technology yet to track....???
> I wonder about that...

Sigh.

✶ 1 Oct 1999 as a Y2K problem date?

David Wittenberg <dkw@cs.brandeis.edu>
Sat, 18 Sep 1999 21:06:17 -0400 (EDT)

Add 1 Oct 1999 to your list of dangerous dates. My Visa bill (which just arrived) is due in early October. The "payment due date" field is apparently too small, so the due date is listed as 0/05/1999. Presumably, the leading digit "1" was dropped.

Why didn't this occur last year? They changed from using a 2-digit year to a 4-digit year in April of this year, and apparently did not realize that they would have to increase the size of the field.

--David Wittenberg dkw@cs.brandeis.edu

[The problem evidently is not at Visa, but rather at David's issuing bank.

It appears to be a format error in the statement printer rather than a

Visa programming problem. PGN]

✉ Re: The real story on Centaur/Milstar (Ladkin, [RISKS-20.57](#))

Marc P <mpassy#nospam#@houston.rr.com>

Thu, 16 Sep 1999 22:12:51 -0500

> Whether or not evidence was present during the launch process,
> how come
> such an error wasn't caught during debugging, inspection,
> component bench
> test, integration test, and all those other things software
> and system
> developers are supposed to do?

For one big reason: This number wasn't present during those phases. One modern space vehicles, these controller gains and constants are dependent on exact vehicle configuration, so they are in file(s) that are loaded into the vehicle during the launch campaign, and require some verification process independent of the original FSW T&V.

In the case of this Centaur problem, the number was specified properly out of the analysis and development group - it was during the manual entry of those numbers into the load file that the error was made. Subsequent verification was not detailed enough to make the error obvious (like launch did), but it was enough to give a few engineers pause. None of them pursued

it with sufficient vigor.

✂ Re: Macro viruses and Word'97's built-in macro detector/ disabler

David Chess <chess@us.ibm.com>

Mon, 20 Sep 1999 14:56:09 -0400

>From: Gisle Hannemyr <lunchbreak@hannemyr.com>

> How technically feasible is it for a macro virus to disable the
> built-in macro detector?

It's utterly trivial; one or two lines of VBA (Visual Basic for Applications, the language that macros are written in in Office'97 and above) can adjust just about any of the adjustable parameters in Word (or any other Office app), including the automatic "this document contains macros" warning.

But of course the virus has to **run** to be able to execute those one or two lines! So if you **never** allow a virus (or any other malicious program) to run, it can't turn off the built-in macro detector (or do anything else). On the other hand, if you accidentally let a virus or Trojan horse run even once, all bets are off, and your system may now have the virus detection turned off. Of course, you can always check; go into the relevant options screen, and make sure "Macro virus protection" is turned on.

Note also that there have been a few flaws discovered that might allow a malicious macro to run without warning, even if you did have the

macro virus protection turned on (see <http://www.microsoft.com/security/> for recent alerts and so on). These have not been generally exploited, but if someone did successfully exploit one, just once, against your system, it might have turned the macro-virus protection off.

DC <http://www.research.ibm.com/people/c/chess/>

✶ Massive hole in NSI web-based e-mail

<root@dotcomnow.com>
19 Sep 1999 19:11:23 -0700

You may be familiar with Network Solutions' recent roll-out of web-based e-mail for domain owners - whether they liked it or not - and subsequent notes that the initial passwords assigned to those accounts were trivially guessable. Unfortunately for NSI, this was not their biggest mistake.

Try this URL:

<http://mail.dotcomnow.com/signup/poll/root>

Congratulations, you can now log in as root. Or this one:

<http://mail.dotcomnow.com/signup/poll/postmaster>

You can now log in as postmaster. This comes about because at the last stage of the new account creation process - after it's checked to make sure you aren't duplicating someone else's account, and created your new one - it

gives you a URL with the username (in cleartext) and password (encoded), so that you can jump right in without logging in. Unfortunately, as you can see here, if you replace that last word in the URL with any account name whatsoever, it will still give you a log-in link with username and password present - you can also jump right in to that account without needing to know the password.

And remember, hundreds of thousands of domain owners just received these accounts, involuntarily. Who do you want to be today? Any domain owner...

<http://mail.dotcomnow.com/signup/poll/pick-a-name>

The Risks? Well, I think the Risks are pretty obvious, no? There's a risk of someone logging in to your root account and sending embarrassing e-mail about your security holes... From: Root, Network Solutions

✶ An easy 'out' for dotcomnow.com accounts (Re: NSI blows it again)

Art Delano <ajd@home.msen.com>
Sat, 18 Sep 1999 10:42:43 -0400

In regards to the massive publicity blow-up which thousands of domain-name holders were notified that e-mail accounts had been set up for them, with login information in plaintext and easily-guessable passwords; I received NSI's spam the evening the scandal broke, apparently identical to the one

which started the brouhaha but without the e-mail account information. Since Slashdot's report implied that accounts had been set up even for people who hadn't been notified, I panicked. So had every other owner of an account in the .com TLD.

I poked around a little. After deciding that there was no account established unambiguously on my behalf, and no security holes compromising anything other than the mail account itself (such as a means to modify domain registration info) I decided not to pursue further. The free e-mail service may have been implemented in stages and halted when the reactions began.

What I did find, though, was the Terms of Service contract at <http://mail.dotcomnow.com/signup/name> (one has to contrive a name to reach the ToS, but can choose to decline the contract after reading it) which states the following:

G. MODIFICATIONS TO AGREEMENT. [...] You may terminate this Agreement at any time by providing us with notice by e-mail addressed to support@nsimail.com or by United States mail addressed to Free Web Mail Comments, 505 Huntmar Park Drive, Herndon, VA 20170-5139.

The agreement, in this case, refers to the contract to which people unwittingly given free e-mail accounts have been unwitting signatories to. (This could lead to the common dilemma of vulnerability to misrepresentation, of course, if somebody decides to arbitrarily cut off somebody else's account in use.)

While Slashdot, with its vast readership, is responsible for fanning the

flames of panic and providing misleading info, NSI is certainly the guiltiest party, in having come up with such a promotion in the first place.

AjD

Long postscript:

Incidentally, NSI offers various free and pay services, all built around and promoted using 'dotcom', in keeping with their slogan, 'the dot com people (tm)'. This led, among other things, to confusion among Slashdot readership -- demonstrated by irate people reporting to Slashdot their efforts to cancel 'dot com mail' (fee-based) accounts which don't exist. Instead of linking to <http://mail.dotcomnow.com/>, the service's front door (which apparently had worked through the peak of the frenzy and is not hosted by NSI), Slashdot's news posting linked to an announcement at <http://www.netsol.com/dotcomnowmail/> and to Network Solution's homepage. During the time NSI's servers were swamped by the slashdot effect, they produced either Page Not Found errors or redirected visitors to NSI's homepage, which promotes 'dot com mail' by name but not dotcomnow.

Adding further confusion to people who might try to guess at URLs and work around the traffic, <http://www.dotcomnow.com/> links to a placeholder page hosted by NSI, while <http://mail.dotcomnow.com/> is the service's proper homepage. No links on the dotcomnow.com pages provide constructive information on who is providing the service, and of the five

links on the homepage, three link to other NSI-hosted dotcom* sites promoting marketing services fuzzily related to dotcomnow.com.

ajd@boutell.com

✂ More data on the NSI spam: acct names and how to change passwords

Lenny Foner <foner@media.mit.edu>

Fri, 17 Sep 1999 18:32:35 -0400 (EDT)

I've got several additional pieces of information about the recent NSI spam.

Executive summary: You probably have accounts you don't know about, and it's impossible to change their passwords securely anyway.

(a) A couple of RISKS subscribers told me, after my plea, that the way to actually get my password changed was to go to mail.dotcomnow.com (rather than directly to the URL present in the spam), and change it there. My thanks to these contributors; this worked. Even better, none of the RISKS subscribers who might have noticed the gaffe in my previous message (in which I inadvertently revealed the account name) took advantage of the situation to change the password -for- me...

(b) The forms for logging in, and for changing one's password, are not encrypted -at all-, e.g., NSI is not using SSL in any way to secure the information in transit. While not as big a breach as is spamming millions

of people with trivially-guessable passwords that will sit in filesystems,
it is still an annoying breach; it means anyone who cares about packet sniffers can't really change their password to anything hard to find, either.

(c) I did some checking around, which is easy, because I have a very unusual last name. In fact, basically all the other Foners in the country, if not the world, are relatives of mine.

The original NSI spam to me claimed that my account name was foner3. However, foner, foner1, and foner2 were also valid accounts, all with passwords of the form "<foo>nsi". [If I've inadvertently changed the password on the account for a relative of mine, the chances are excellent, based on past experience, that they read RISKS as well, so let me know, okay?] Interestingly enough, I am definitely the very first Foner to have ever created any records in the DNS (by many years), so it's interesting that the only one that got any mail was foner3. (And most of my e-mail addresses, even from 20 years back, still get to me, so it's not likely that they got lost in transit.)

On the other hand, I own two domains, for which the NIC handle is LNF2. (I also used to administer a domain, ten years ago, for which my NIC handle is LNF1. I have never been able, in a couple of years of trying, to get NSI to actually merge these two records---they seem to have absolutely no procedure for handling this. Filling out their forms causes automated

bounces;

"scribbling" all over the margins with a text editor (in the rightmost columns, etc) saying "PLEASE HAVE A HUMAN BEING READ THIS AND DEAL WITH IT"

causes the forms to be black-holed. Thus, there is now a dangling pointer in their database about who actually administers this ten-year-old domain for a company that I used to work at, and there are two similar but conflicting records about how to contact me, one of them wrong by ten years.

Typical NSI. I also find it curious that domains have last-modified and created-on-date information, but NIC handles only have last-modified.)

Neither LNF1 nor LNF2 are valid e-mail accounts in the dotcommail system; I just tried them. I have no idea why there are -four- listings for my last name in the system. (I tried foner0 through foner7 and then ran out of enthusiasm for the project; I'm reasonably sure they only went up to foner3. There are 6 Foners listed in the NIC WHOIS database, so that ain't it, either.)

-However-, "yenta" (with password "yentansi") -was- a valid account; I own YENTA.ORG. On the other hand, I own ECM.ORG, and "ecm" was -not- a valid account. (Neither were yental, ecml, etc.)

P.S. Needless to say, my passwords for all of these accounts are now concatenations of various unprintable epithets relating to the ancestry and intelligence of NSI and its employees. And if anyone ever receives any mail from me from any of these accounts, you must presume that it is

nonetheless
a forgery unless you have confirmation through some other
channel that it is
not.

⚡ Final bit of info re NSI spam

Lenny Foner <foner@media.mit.edu>
Fri, 17 Sep 1999 19:02:42 -0400 (EDT)

I just discovered (after sending the previous mail) that the way
to figure
out who the account thinks it's for is to log in, go to the
Preferences
page, and then go to the Personalities page. This tells me, for
example,
that my "duplicates" are relatives: "foner" is Carl, "foner1"
and "foner2"
is Joel (twice? hmm), and "foner3" is me---and that "yenta" was
Larry Yenta
(oops!). I'm sending them all mail explaining what happened...

Interestingly enough, they're all of the form "Leonard foner", e.
g., the
last name is not capitalized.

P.S. Anyone want to hazard a guess as to why "whois yenta" shows
Larry Yenta's entry, and yenta.com (not mine), but not yenta.org
(which -is- mine)?

[I've a yen ta duck that one. But in response to someone
else's query,

a comment from Lauren Weinstein leads me to suggest that you
might try

<http://www.geektools.com/cgi-bin/whois.cgi>

, which can give you non-NSI domain assignments as well. It
says it

is a "Work in progress", but it appears to be a valuable one.

PGN]

✉ Re: NSI blows it again (Foner, [RISKS-20.58](#))

Brian Clapper <bmc@WillsCreek.COM>

Tue, 21 Sep 1999 13:47:26 -0400 (EDT)

Lenny Foner describes the recent Network Solutions spam and free e-mail account debacle. On that same topic, CNET reports that "e-mail hosting provider Critical Path has acknowledged a serious security hole that compromised accounts within services offered by a number of customers, including Network Solutions, the dominant domain name registrar."

"The hole is similar to one that plagued Microsoft's Hotmail last month by allowing access to a user's account without requiring a password first. The more recent breach, which Critical Path confirmed yesterday, comes as Network Solutions (NSI) is offering new services such as free e-mail to hold on to customers who may be lured away by new competitors.

"Critical Path, which provides behind-the-scenes resources for activating accounts on NSI's new service, said the problem affected other free e-mail clients but declined to name them."

See "<http://news.cnet.com/news/0-1005-200-121667.html>" for details.

This ill-implemented Network Solutions promotion illustrates a larger risk:

How competent is Network Solutions? The RISKS archives are filled with

examples of Network Solutions screw-ups (see [1] through [5], below). Of course, one can argue that these are isolated problems, and that Network Solutions is doing a relatively good job day-to-day. However, my personal experience with them in recent years has left me unimpressed with their competence. I have had problems with their PGP key server (most recently, they somehow lost my PGP key, causing my submitted change requests to fail mysteriously until I determined that I had to register the key again), trouble with their telephone support (which I've never found to be particularly helpful, on those rare occasions I've managed to get through at all), and a few apparently lost change requests. And as for their customer service, I'm highly unimpressed: While attempting to resolve such problems, I've found it nearly impossible to get in touch with an actual person (competent or otherwise), whether by phone or by e-mail.

Yahoo has the unaudited income statement for Network Solutions, for the first half of this year. (See <http://biz.yahoo.com/fin/19990816/nsol/ti.html>)

It lists their gross revenues at (US) \$85,631,000 (with a net profit of \$10,593,000 for the same six months). That's more than double the revenue for the same period last year. Some analysts are projecting that Network Solutions will grow 40% over the next three years. With that kind of rosy business outlook and current revenue stream, it's a little difficult to understand why their customer service is so poor--other than their all-but-monopoly status as a domain registrar.

I'm encouraged that the Commerce Department has been experimenting with competition for Network Solutions (see, for example, <http://news.cnet.com/news/0-1005-200-116634.html>). Hopefully, competition will also cause them to improve their service--or, at least, provide customers with workable alternatives.

- Brian Clapper, bmc@WillsCreek.COM

[1] Rodger, Will. "Network Solutions goof bumps NASDAQ off the Internet."

RISKS Forum Digest, Volume 19, Issue 34, 26 August 1997.

[2] Moran, Douglas. "'Unfixable' error in InterNIC database."

RISKS Forum Digest, Volume 19, Issue 77, 30 May 1998.

[3] Kamens, Jonathan I. "The InterNIC: a case study in bad database

management." RISKS Forum Digest, Volume 18, Issue 67, 13 December 1996.

[4] Perry, Elizabeth Hanes. "Bring me the head of InterNIC."

RISKS Forum Digest, Volume 18, Issue 92, 20 March 1997.

[5] Pouzzner, Daniel "Partial failure of Internet root nameservers."

RISKS Forum Digest, Volume 19, Issue 25, 18 July 1997.

✉ Re: 22nd National Information Systems Security Conference

"Ed Borodkin" <borodkin@constitution.ncsc.mil>

Tue, 21 Sep 1999 12:40:01 -0400

22nd National Information Systems Security Conference
Hyatt Regency, Crystal City
located just 5 minutes from downtown Washington, DC

October 18-21, 1999

As a leading global forum on computer and information systems

security,

the National Information Systems Security Conference seeks to:

- bring together information security and technology

professionals from

industry, academia, and government;

- provoke debate, dialogue, and action on major information security

issues for today and tomorrow;

- educate the IT community on major information security issues and

solutions;

- promote demand and investment in information security products, solutions, and research;

- challenge the IT community to provide solutions, research, and applied technology that are usable, inter operable, scalable, and affordable.

See <http://csrc.nist.gov/nissc/> for the program and registration instructions.

nissconference@dockmaster2.ncsc.mil

Registration information: (301) 975-3883

Program information: (410) 850-0272

Ed Borodkin, Program Director, NISS Conference

✶ 15th ACSAC Advance Program

Vince L. Reed <vreed@mitre.org>

Fri, 17 Sep 1999 15:13:47 -0500

The conference committee for the Annual Computer Security Applications

Conference (ACSAC) is proud to announce the 1999 Advance Program, 6-10

December 1999, in Phoenix Arizona. It is available on the world wide web

at: <http://www.acsac.org/>.

Vince Reed, CISSP

Publicity Co-chair

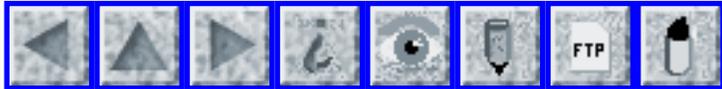
Annual Computer Security Applications Conference

1500 Perimeter Pkwy., Suite 310, Huntsville, AL 35806-3578

Phone: +1.256.890.3323, FAX: +1.256.830.2608

publicity@acsac.org

<http://www.acsac.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 20: Issue 60

Monday 27 September 1999

Contents

- [Ikonos launched successfully](#)
- [Computer problems foul up the Washington Metro system](#)
[Steven M. Bellovin](#)
- [Faulty aircraft collision avoidance system RISKS causing collision](#)
[Mike Martin](#)
- [Net users "page-jacked" by pornographers](#)
[NewsScan](#)
- [Wonder when automatic toll-taker transponders will be cracked?](#)
[Jim Warren](#)
- [You don't even need a computer ...](#)
[Rob Slade](#)
- [Re: UK rail disaster](#)
[Clive Page](#)
- [9/9/99?](#)
[Joseph A. Dellinger](#)
- [The Microsoft/NSA Crypto Brouhaha](#)
[mp](#)
- [my.Yahoo.com bug/risk...](#)
[Matt Anderson](#)
- [Risk of being removed from a spam list!](#)

[Marc Salverson](#)

- [Mars Lander reprogramming](#)
 - [Re: Loss of Mars Climate Orbiter](#)
[Lord Wodehouse](#)
 - [Re: Mars Pathfinder a failure?](#)
[Steve VanDevender](#)
 - [Re: Mars Pathfinder](#)
[Ben Hines](#)
 - [Re: Mars Climate Observer](#)
[Harlan Rosenthal](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ **Ikonos launched successfully**

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

Mon, 27 Sep 99 8:56:57 PDT

The first successful launch of Space Imaging's Ikonos satellite occurred on 24 Sep 1999, from a Lockheed-Martin Athena II, following the earlier failure on 27 Apr 1999 ([RISKS-20.36](#) and [38](#)) -- which has been blamed on an electrical problem that prevented the aerodynamic payload covering from coming off. Ikonos provides one-meter resolution, and is intended for public consumption.

✶ **Computer problems foul up the Washington Metro system**

"Steven M. Bellovin" <smb@research.att.com>

Fri, 24 Sep 1999 14:21:59 -0400

According to the AP, the 3-year old \$20M central computer system

that monitors the position of every train in the Washington, D.C., Metrorail system failed on the morning of 24 Sep 1999. The backup involved personnel with walkie-talkies along 96 miles of track monitoring trains. As a result, the morning startup was delayed by half an hour.

[The cause was not identified. But this was reportedly the first time in

23 years that the start of daily service was delayed!

"A graphics generating device for Metro's finicky central computer

system froze about 3:20 a.m., sending Metro managers racing to fix it

before the scheduled start of daily service at 5:30 a.m. But they

couldn't restore it until 5:46 a.m., which meant normal passenger

service didn't begin rolling until about 6:15 a.m." -- resulting in

45-minute delays to start the day. "Last fall, the system crashed

several times during rush hour, including one episode similar to

yesterday's when computer-generated views of sections of the system were

blacked out for nearly two hours. In the 15 months after the system was

installed by McLean-based BDM International, it crashed 50 times."

Source: Computer Failure Puzzles Metro Opening Delayed, Rush Hour

Slowed, by Lyndsey Layton, *The Washington Post*, Saturday, September 25,

1999, Page B01, courtesy of Keith Rhodes; PGN-ed

<http://www.washingtonpost.com/wp-srv/WPlate/1999-09/25/0741-092599-idx.html>

✈ Faulty aircraft collision avoidance system RISKS causing collision

"Martin, Mike" <mmartin@sbns.com.au>

Mon, 27 Sep 1999 16:08:17 +1000

The Australian Bureau of Air Safety Investigation recently made recommendations (<http://www.basi.gov.au/rec/r19990156.htm> <<http://www.basi.gov.au/rec/r19990156.htm>>) following two incidents where aircraft traffic alert and collision avoidance systems (TCAS) gave faulty altitude readings.

The first case, which occurred near Hawaii in January 1998, involved a B747 and a DC8. Although the aircraft actually had 2000 feet vertical separation, the TCAS unit in the lower aircraft reported it to be 1500 feet higher than it actually was, presaging an evasive manoeuvre. Fortunately Hawaii air traffic control noticed the discrepancy between the altitude reported by the transponder and the altitude reported by the crew. Matters were then sorted out without risk to either aircraft.

The same BASI report also discusses a more recent incident in Chinese airspace last June, when two B747 aircraft almost collided at 31,000 feet. Malfunctioning TCAS equipment resulted in the higher altitude aircraft descending towards the lower one.

In neither of these cases did the crew have any on-board means of knowing what altitude their TCAS was signalling and thus no means of realising that it was malfunctioning.

While TCAS technology is a valuable contribution to safer skies, its malfunction can introduce new risks. These are exacerbated when air crew have no on-board means of knowing whether the equipment is working correctly or not.

The BASI report on the second incident observes, "[it] placed both the aircraft involved and all on board at very high risk... Ultimately, it was only the 200 m lateral separation that prevented a mid-air collision, and this separation was not provided by TCAS avoidance manoeuvres."

It later goes on to observe, "With TCAS only able to provide separation in the vertical sense or, perhaps more importantly in this case, decrease separation in the vertical sense, it would seem appropriate to provide additional lateral separation. Had the aircraft in this incident each being flying 1 NM right of track, the ensuing separation (assuming the events would still have occurred) would have been 2 NM. Offset tracks such as this are operated in some airspace where air traffic control may not be as effective as desired but this incident was not caused by ineffective air traffic control."

There has been previous discussion in RISKS about increasingly precise aircraft navigation leading to increased risk of mid-air collision ("Air collision RISK from increased accuracy", John Brooks, [Risks 19.07](#)).

These two incidents illustrate the reality of this.

The BASI article makes a number of recommendations aimed at

reducing the
risk from faulty TCAS equipment.

Mike Martin, Sydney Mmartin@sbnsw.com.au

⚡ Net users "page-jacked" by pornographers

"NewsScan" <newsscan@newsscan.com>

Thu, 23 Sep 1999 09:11:31 -0700

American and Australian investigators have zeroed in on an elusive Portuguese cracker and an Australian pornography company as the perpetrators of a fraudulent scheme to "page-jack" would-be visitors to legitimate Web sites, such as the Harvard Law Review, and transport them to online porn sites. The users reported that the only way they could escape was to shut down their computers and reboot. Attempting to use the "back" or "home" buttons merely resulted in being subjected to more pornography. Investigators say the page-jackers were able to steal viewers by copying legitimate Web pages and their so-called metatags, which provide key words and code that are used to index the site for search engines. Australian officials are considering civil or criminal charges against the company, and a federal judge in Virginia has ordered many of the sites run by the company off the Web, and directed the perpetrators to stop copying legitimate Web pages. Executives at Alta Vista, which was used for the scam, say that the search engine has taken steps to correct the problem by carefully monitoring their index and by offering filters that can screen out

pornography. (*The
New York Times*, 23 Sep 1999; NewsScan Daily, 23 September 1999,
reproduced
with permission; original at
[http://www.nytimes.com/library/tech/99/09/biztech/
articles/23fraud.html](http://www.nytimes.com/library/tech/99/09/biztech/articles/23fraud.html))

✶ Wonder when automatic toll-taker transponders will be cracked?

Jim Warren <jwarren@well.com>
Sat, 25 Sep 1999 13:28:20 -0700

As some people know, various states' Transportation Departments and various toll-bridge and toll-road jurisdictions have begun to deploy various kinds of automated toll-collection systems. These involve having some kind of transponder in or on the vehicle. This may be a small device the the driver places near the front windshield when approaching a toll plaza. Other systems require that the device be mounted on the vehicle, usually inside the front grillwork.

As the vehicle approaches the toll plaze, equipment installed in the toll plaza can sense these transponders, identifying the vehicle (or, at least, the unique transponder) without the driver ever needing to stop or hand over cash. Typically, drivers using these systems deposit funds, from which the toll fees are automatically deducted as the transponder passes through the toll-plaza sensor.

The question is: When will these devices be cracked and cloned -- just like the massive cloning racket that is done with cell-phones?

Think it's not worth it? Think again! Remember -- Capt'n Crunch was one of the first who was caught, prosecuted and convicted of cracking [San Francisco] Bay Area Rapid Transit (BART) magstripe tickets, 10-20 years ago!

Of course, the risk will be greatly increased for those toll systems that require that the transponder be permanently turned on -- rather than turning it on only as one nears the toll plaza. Then, any cracker sitting on any approach leading to a toll plaza should be able to trigger it and/or pick up the transponder's id, for later cloning.

The safest toll systems will allow the driver to completely shield, or otherwise turn-off, their transponder -- except when they are almost actually inside the toll-plaza's vehicle-slip. (But of course, this makes the transponders useless for law enforcement that may want to be able to sense the transponder, far distant from the toll plaza ... for speed enforcement and other possible covert surveillance purposes. :-)

Just another [paranoic] thought about crackers, law enforcement and the "wonders" of technology. (Just because I'm paranoid doesn't mean that ... :-)

jim, Jim Warren, jwarren@well.com, GovAccess list-owner/[im] moderator/janitor
345 Swett Rd, Woodside CA 94062; 650-851-7075; fax-for-the-
quaint/650-851-2814

⚡ You don't even need a computer ...

Rob Slade <rslade@sprint.ca>

Thu, 23 Sep 1999 13:29:53 -0800

I hit my first carbon-based Y2K bug yesterday.

My wife was given a gift certificate for a restaurant last month (August: you'll figure this out shortly) and we finally got around to trying out the restaurant this week. (Quite nice.)

When the time came to pay, we presented the gift certificate. The waitperson took it away, but returned almost immediately to tell us that it was no good: it had expired. Sure enough, there was an expiry date: July 31st, 00. Actually, Gloria is better at this than I am: she was the first one to figure out what was wrong, and to explain that, obviously, the 00 stood for 2000, and the certificate was good for almost a year yet. The waitperson still wasn't sure about this, and went to check, but obviously got told that it was OK.

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

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

⚡ Re: UK rail disaster (Lyons, [RISKS-20.59](#))

Clive Page <clive@page.demon.co.uk>

Fri, 24 Sep 1999 22:23:03 +0100

>... The train was also fitted with Automatic Train Protection (ATP),
>but this was also switched off ...

One of the accounts that I read said that the ATP could have been switched on when this driver took over, but that it took four minutes to warm up, during which time the train had to be stationary, and no-one wanted to make the train late. No doubt the designers of the device thought that it didn't matter much that it took so long to warm up (just as Microsoft doesn't have much incentive to make Windows boot up in much less than one minute) but clearly a device with a slow start **does** have safety implications, if it someone has the choice of not using it in order to save time.

Clive Page

✶ 9/9/99?

"Joseph A. Dellinger" <jdellinger@amoco.com>

Wed, 22 Sep 1999 17:15:23 -0500 (CDT)

The Wall Street Journal seems to have reported that 9/9/99 was a nonevent.

Yet, a relative of mine was shocked to discover \$160K inexplicably credited to their account. When they went to the bank to get it corrected, they found a line of people already there waiting to see the bank officers. The person in front of them in line had done considerably better: they had

received
over 2 million dollars that way. The transactions had occurred
on September
8, and the statement with the errors on it was printed September
9. The
bank (a well known name) "thanked them for their honesty in
coming forward",
"apologized for the inconvenience", "had already fixed the
problem so it
wouldn't happen again", and "advised all their customers to hold
on to all
paper statements". This event (which apparently affected at
least several
dozen people in a Dallas suburb) went entirely unreported in the
local
media.

Was this the (mythical?) 9/9/99 bug or an unrelated fluke? I
certainly never
heard of something like this happening before to anyone I
personally knew!

✦ **The Microsoft/NSA Crypto Brouhaha (Re: Wallach, [RISKS-20.58](#))**

mp <mp@the-wire.com>

Sat, 25 Sep 1999 12:53:27 -0400

> Microsoft has said in public that
> this is a "backup" key, which is also believable.

Not really. Microsoft argued that a secondary key was needed in
case the
primary signing key was somehow lost. This is a danger, but
there is no need
to introduce a secondary key when they can just as easily keep a
secure
off-site copy of the primary key. (There are good reasons to
have a

secondary encrypting key, but this was a signing key.)

A secondary signing key could be useful because it could allow the primary key to be revoked if it was somehow compromised. Unfortunately Microsoft's system does not support key revocation. Microsoft's system does not even inform the user which key was used to sign the CSP module.

I think a large part of the concern is due to the fact that a secondary key makes it easier for an attacker to replace one crypto module without anyone noticing.

⚡ my.Yahoo.com bug/risk...

Matt Anderson <manderson@hopeconsulting.com>

Fri, 24 Sep 1999 15:14:11 -0400

Recently I had an opportunity to borrow an old laptop of a co-worker for use on a business trip. While on the trip, I used the Netscape browser (4.x) on the laptop to access the internet. The browser was set to my co-worker's web page, my.yahoo.com. Being a bit mischievous, I added a few things that got displayed on his web page(He got back the latest news on the goings on of Cricket, NASCAR, Boxing and the LPGA). My co-worker (who uses IE5.0) discovered this right away using his new computer and changed his password. However, I was still able to access his web page and modify his profile. Even after an extended period of time(overnite) and with the old laptop turned off, when I powered the laptop up and started up the

Netscape

browser, I was still able to access the web page the following morning.

Needless to say, when I found out that my co-worker had changed the password

3 times and I still could access it, we recognized it as a security hole in Yahoo's website.

We were able to recreate this repeatedly. It is rather simple.

Go to

my.yahoo.com in your Netscape browser and create a yahoo account and check

the box that says remember password and id. Then exit the Netscape browser.

Now start a IE browser and go to the same URL(my.yahoo.com) and type in your

account_id and password and check the box that says remember password and

id(as a cookie). Change your password via the IE5.0 browser.

Now bring up

your Netscape browser and go to the same URL(my.yahoo.com)

again. You still

get into the web page.

Whether this is a combo Netscape/Yahoo problem or just Yahoo remains to be

seen. Yahoo techies basically blew us off with suggestions like "cache

retention" and proxy server page caching. But it would seem obvious to me

that both suggestions are without merit as they would imply that we should

simply get the same page back again and we were getting updated news items

and the pages would differ as we updated them. Of course it also doesn't

explain how you could add sections and delete sections of a web page and

cache memory would know how to do that.

While the risk is limited(I couldn't access his e-mail or add him to yahoo

mailing lists, however I didn't explore all the possibilities) and I also didn't explore what possibilities existed with other websites (Amazon comes to mind with their one-click purchase options), however, the obvious potential is there for more malicious attacks from more mischievous co-workers than myself. Basically, any one who grabs your cookie.txt file can get access to your web page REGARDLESS OF HOW MANY TIMES YOU CHANGE YOUR PASSWORD.

Any web site that assumes the identity of the user even if its only at the surface, leaves itself more vulnerable than those that do tighter security checks.

M@ Anderson, Chief Engineer, Hope Consulting Group, Inc. www.hopeconsulting.com
88F Jefferson Boulevard, Warwick, RI 02888 (401) 785 - 3211

⚡ Risk of being removed from a spam list!

Marc Salverson <marC@undergraph.com>

Thu, 23 Sep 1999 09:31:55 -0500

The dot com free e-mail spam from Network Solutions includes:

- > If you do not wish to receive e-mail from Network Solutions, click on
- > this e-mail address <<mailto:netsolremove@integram.org>> and type
- > "remove" in the subject line.
- > PLEASE NOTE: by opting to be removed from this list we will not be
- > able to communicate to you, in real-time, on issues regarding your
- > account.

So, what they're saying is that if they decide to set up free e-mail for you, with an easily guessable password, they won't tell you?

Oh, what a Risk!

Marc Salverson <marC@undergraph.com>

⚡ Mars Lander reprogramming

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

Mon, 27 Sep 99 9:01:15 PDT

After the loss of the Mars Polar Orbiter ([RISKS-20.59](#)), the Mars Polar Lander is being reprogrammed to report its data directly back to earth. The Lander is scheduled to reach Mars on 3 Dec 1999. Stay tuned.

⚡ Loss of Mars Climate Orbiter

Lord Wodehouse <w0400@ggr.co.uk>

Thu, 23 Sep 1999 20:05:00 +0100

From the reports so far, it appears that Mars Climate Orbiter flew too close to Mars (60Km) as opposed to about 140Km. 60Km is considered 25Km below the minimum safe height.

BBC online news has a quote from JPL:

"Yesterday, MCO was approaching the planet to pass within 140km of the surface and all seemed okay. However, in the last six to eight

hours

before the approach we saw a 100km drop and we don't understand why."

Now 100Km changes don't just happen, so the question is "Where was the error in the calculations?" Somewhere either a tracking error or software error has gone unnoticed until too late, or the final correction burn was not as expected.

However the knock-on of this mistake is going to be a real issue. Mars Polar Lander and the two Deep Space 2 microprobes depended on having Mars Climate Orbiter to relay data from them to Earth and also to relay commands back. So "smaller, cheaper, faster" has hit a snag, which was not allowed for. NASA will no doubt say it can recover, but with the budget cuts, this will not be easy.

Past errors like the HST mirror, Galileo's high gain disk and the loss of SOHO were recoverable, because either clever engineering and/or great innovation (especially operating SOHO with no gyros at all) have proved possible. But the demise of MCO seems reminiscent of Icarus! Too close is always a one way ticket! --

Global Research Information Systems, Glaxo Wellcome Medicines
Research Centre
Tel: +44 (0)1438 76 3222 <mailto:w0400@ggr.co.uk> (preferred)

✶ Re: Mars Pathfinder a failure?

Steve VanDevender <stevev@efn.org>

Fri, 24 Sep 1999 00:20:53 -0700 (PDT)

... The U.S. lost a 1993 Observer,
and more recently the Mars Rover Pathfinder ([RISKS-19.49](#) to
[56](#)). There
have of course been some successes, with the Viking landers
(1970s) and
Pathfinder (1997).]

I'm a little confused by PGN's contradictory statements
regarding Mars
Pathfinder above. At least according to all the NASA statements
I saw, the
Pathfinder lander lasted almost 90 days before it stopped
communicating with
Earth, but had a design lifetime of only 30 days; the Sojourner
rover only
needed to last about a week to meet its mission objectives but
was still
working well when the lander failed, cutting off the ability to
relay
communications to and from the rover. (This may very well have
left
Sojourner slowly circling the lander until it too failed, as
that was the
rover's programmed contingency plan if it lost communications
with the
lander.) As a relatively inexpensive mission Pathfinder was
intentionally
not designed to last indefinitely on the Martian surface, and it
was
expected that thermal cycling would eventually fracture
connections in the
lander's electronics.

While the priority inversion problem in the Pathfinder lander's
software
that caused spontaneous reboots was irksome and extensively
discussed in
RISKS as an example of the difficulties of real-time OS
scheduling, it was
by no means fatal to the mission.

If navigational error is considered to be the most probable cause of the Mars Climate Orbiter's loss, this will be a rare sort of failure for NASA.

I cannot recall any NASA interplanetary probe previously being lost due to gross navigational problems, and many of those are in far more distant and complicated environments, such as the Galileo probe's lengthy stay at Jupiter involving many close passes to the Galilean moons and a continuously-changing orbit. Mars Global Surveyor was even successfully aerobraked into its desired orbit despite a greatly extended period of aerobraking to avoid additional damage to a weakened solar array, which required careful monitoring of its status and frequent adjustments to its orbit for over a year.

✶ Re: Mars Pathfinder

Ben Hines <bhines@san.rr.com>

Thu, 23 Sep 1999 19:46:31 -0700

PGN said in [RISKS-20.59](#) that the US lost the "mars rover pathfinder".

In fact, the Rover was called Sojourner. The mission and lander itself was called Mars Pathfinder. And indeed, they did lose the signal, but after over 3 months of ground time - for a mission designed for a month long stay.

Pathfinder has never been considered a failure.

bhines@san.rr.com <<http://members.tripod.com/~tunnels/>>

⚡ Re: Mars Climate Observer ([RISKS-20.59](#))

Harlan Rosenthal <Harlan.Rosenthal@Dialogic.com>

Fri, 24 Sep 1999 09:00:19 -0400

>>Mars has been a tough target.

That's because the Martians keep shooting things down.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 61

Friday 1 October 1999

Contents

- [English or Metric - why Mars Climate Orbiter was lost!](#)
[Lord Wodehouse](#)
- [Japanese Nuclear accident: a case study of bad design](#)
[Chiaki Ishikawa](#)
- [Massive Fiber Cut Pauses East-West Traffic](#)
[David Farber](#)
- [FBI warns some Y2K fixes may be suspect](#)
[NewsScan](#)
- [Misreading and nuclear war -- or not](#)
[Simon Hogg](#)
- [Internet Explorer 5.0 flaws](#)
[Steve Wildstrom](#)
- [Elliptic curve 97-bit challenge broken](#)
[Dorothy Denning](#)
- [Intuit "Shuts Down" Privacy Site After PRIVACY Forum Query](#)
[Lauren Weinstein](#)
- [Henry Petroski, books, and risks of technology](#)
[PGN](#)
- [Linux banned after Samba misconfiguration blocks NT authentication](#)
[B. W. Fitzpatrick](#)

● [Cyber-Speak](#)

[Ira J Rimson](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ English or Metric - why Mars Climate Orbiter was lost!

Lord Wodehouse <w0400@ggr.co.uk>

Fri, 01 Oct 1999 20:07:30 +0100

The following quoted from NASA's press release shows that for the second time a mix-up in units resulted in an experiment failure, but this time it was a spacecraft.

> The peer review preliminary findings indicate that one team
> used English units (e.g., inches, feet and pounds) while the
> other
> used metric units for a key spacecraft operation. This
> information was critical to the maneuvers required to place the
> spacecraft in the proper Mars orbit.

>
> "Our inability to recognize and correct this simple
error
> has had major implications," said Dr. Edward Stone, director of
> the Jet Propulsion Laboratory. "We have underway a thorough
> investigation to understand this issue."

Risks - too many to list, but if after 40 years NASA can't sort out measurement units, what hope have we for Starwars projects. It is a terrible inditement to have to admit to. It certainly ranks with the HST mirror as a fiasco.

Perhaps Europe has got it right for once. Metric units at least mean factors of ten or more out, which tend to show up errors. The English still have miles and pints and galleons (UK not US), but they do their

science in
metric units.

Global Research Information Systems, Glaxo Wellcome Medicines
Research Centre
Gunnels Wood Road, Stevenage SG1 2NY UK +44 1438 76 3222
w0400@ggr.co.uk

[Thanks to all of you, too numerous to cite, for noting this
item.

The measure in question was apparently kilograms per second
vs. pounds per
second of force, off by a factor of 2.2, which would seem to
explain the
too-close approach. The need for very strong typing strikes
again. PGN]

🔥 Japanese Nuclear accident: a case study of bad design

Chiaki Ishikawa <Chiaki.Ishikawa@personal-media.co.jp>

Fri, 1 Oct 1999 04:34:00 +0900 (JST)

By now, many of you are aware of the Japanese nuclear accident
where a large
amount of Uranium solution was placed in one condensation
container and
achived the "critical" condition for runaway fission and thus
released
high-energy particles (and heat) and generally radio active
materials.

For example,

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

has an article titled "Radiation Leak in Japan".

Already the incident seriously injured three people and 21 more
people were
exposed to high dose of radiation. (The number of people found
to be

exposed has been increasing over the last few hours.)

That a certain amount of Uranium solution would reach such critical condition has been known for years. For example, Richard Feynmann's "Surely you are joking, Mr. Feynmann" chronicles the author's experience of seeing a rather sloppy handling at Oak Ridge laboratory where the army people were not aware that the water solution needs much smaller amount of Uranium to reach the critical condition than solid or powder since water acts as a slowing material and increases the chance of neutron's interaction with Uranium and such. Feynmann and his superior Segre(spelling?) explained the basics of the nuclear material and how to calculate the critical mass (of solutions) in order to work out the practical avoidance guideline. This happened before the atomic bombs of 1945.

So, WHY ON EARTH, in today's fuel processing facility, such concentration of Uranium solution can happen or is allowed to happen?!

According to a news article (in Japanese) at Mainichi Shimbun newspaper site

<http://www.mainichi.co.jp>

a few bad design and operation decisions emerge.

First, there was no strict oversight of the line operators who moved the solution during a condensation process. The operators move the solution to a large condensation tank from a container. But, there is no checking mechanism that the critical amount of uranium is deposited in this condensation tank. It seems that the reckless handling of the solution

marginally below the limit was routine (I may be wrong. I hope I am wrong, but the article seems to suggest that this was the case.)

It is reported about 7 times as much solution allowed was dumped by mistake. Agah.

Furthermore, the designers and management people of the processing plant don't seem to believe in Murphy's Law.

There was no automatic warning or similar when the amount of over the allowed amount (below the critical amount of course) is thrown into the condensation tank. So there was no incentive to the line operators not to go over the threshold carefully. (Weren't they taught about basics?!).

No procedural manual exists to handle such "critical condition" event, should it happen.

The three operators who directly caused the incident were found lying on the floor when three colleagues entered the area after hearing the siren warning the high radiation level.

The village people near the plant was furious since they were not notified promptly. They learned the accident TWO (2) hours after the incidence: by then, radiation material escaped the building. A clearly written well prepared manual at least could have warned these people much quicker. After all, the plant people had the time to check out radiation level outside the plant around 11:45 am. The village people were notified around 12:30. The

accident was believed to have happened around 10:35 am.

Aside from the three people, the plant workers in the next buildings were found to be exposed to large dose and some small radio active particles were found in some people's hairs.

Oh well, as of now at 3 am in the morning, the local provincial government where the plant is located shielded off 350 meters radius area (it seems that it is being extended to 500 meters as I write this post now.). People living in the 10 km radius, (310,000 people) are being advised not to go outside until tomorrow morning (as if something would happen by then.).

A few bad designs indeed. Why don't people get things right, what the people back in the 1940's managed to handle?

I have had some bad things to say about the Japanese nuclear power industry. I have no idea HOW these guys would continue operating in this manner. We need a Saturday night massacre style of shuffling of heads and inject some sense of scientific integrity to the newly hired workers and management, I guess.

That a renowned nuclear physicist turned politician, Dr. Arima is in charge of the government agency overseeing the industry could be a good omen. However, if he can handle the guys with such shoddy history behind them in the industry effectively in a short time is a question. In any case, Dr. Arima was quickly assigned the chair of the ad-hoc overseeing committee yesterday.

I bet criminal investigation would commence for the plant operators and such. (I wish it does.)

PS: Right now, the water container that surrounds the condensation tank is being emptied. I hate to think who is/are doing this where. The water surrounding the condensation tank is believed to act as "mirror" for the neutron particles that cause the runaway fission. By emptying the water tank, it is hoped that the neutrons are no longer reflected back to the condensation tank and fission somehow subsides.

Oh, I forgot to mention. After more than 12 hours, it seems that the critical condition still continues!. Counts of neutron has been high meaning that the runaway fission in small scale continues. (But not much dust particles seem to be blown into the air.)

Can we call this a micro-Chernobyl? It's up to you.

I am not sure if the reported better preparedness of a currently planned processing plant in Aomori (the northern part of Honsyu island) against this type of accident is a blessing or too little too late.

Chiaki Ishikawa <ishikawa@personal-media.co.jp.NoSpam>
Personal Media Corp., Shinagawa, Tokyo, Japan 142-0051

[slight spelling corrections, including one in archive copy.
PGN]

Massive Fiber Cut Pauses East-West Traffic

David Farber <farber@cis.upenn.edu>

Wed, 29 Sep 1999 17:17:49 -0400

[from Dave's IP distribution]

Massive Fiber Cut Pauses East-West Traffic

Click on our sponsors! Updated 11:42 AM ET September 29, 1999By
Max

Smetannikov, Inter@ctive Week

At least four Internet service providers are experiencing severe
traffic

backlogs because of a massive fiber-optic cable cut that put out
four OC-192

lines connecting data networks on the East and West Coasts.

Industry

sources told Inter@ctive Week that the cut was accidentally made
by an

unidentified gas company in Ohio around 12:30 EST today.

The news is sending shockwaves through the networking community,
with many

carrier operators struggling to understand why, all of a sudden,
their

traffic is routed through London and Denmark. At least four
Internet service

providers are being affected by the outage. Various online
sources have

named AboveNet; GTE Internetworking; and MFS Communications, a
WorldCom

subsidiary, as ISPs hit the worst.

"Let me tell you, it really hurts right now," said Dave Rand,
AboveNet's

chief technology officer. "We were given a 1 hour estimate for
this problem

to be corrected."

GTE Internetworking's public relations department had heard of
an outage in

Pennsylvania earlier today, but had no comment on the Ohio

development. MCI

WorldCom public relations didn't have an immediate answer to the query.

[The cut apparently resulted from gas company workers during construction.

Various ISPs were still down hours later. PGN]

✶ FBI warns some Y2K fixes may be suspect

"NewsScan" <newsscan@newsscan.com>

Fri, 01 Oct 1999 06:10:52 -0700

The Federal Bureau of Investigation says that some of the Y2K-related programming fixes that were undertaken by foreign contractors may contain malicious code. "We have some indications that this is happening," says Michael Vatis, head of the inter-agency National Infrastructure Protection Center. "A tremendous amount of remediation of software has been done overseas or by foreign companies operating within the United States." A Central Intelligence Agency officer assigned to the Center said recently that India and Israel appeared to be the "most likely sources of malicious remediation" of U.S. software. "India and Israel appear to be the countries whose governments or industry may most likely use their access to implant malicious code in light of their assessed motive, opportunity and means," CIA officer Terrill Maynard wrote in the June issue of Infrastructure Protection Digest. Such code could contain "time bombs" set to detonate at some future date, disrupting service or compromising security

and password

protections. The Special Senate Y2K committee, in its final report last week, called such scenarios "unsettling." (Reuters/TechWeb 1 Oct 99)

<http://www.techweb.com/wire/story/reuters/REU19991001S0001>; NewsScan Daily, 1 October 1999, with permission)

[See also http://dailynews.yahoo.com/h/nm/19991001/tc/yk_code_2.html . PGN]

✶ Misreading and nuclear war -- or not

Simon Hogg <s.hogg@freeuk.com>

Fri, 01 Oct 1999 12:36:48 +0100

I get a 'digest' of 'interesting' news stories once a month from a computer magazine here in the UK (not that interesting, but I have never gone to the trouble of cancelling the subscription). Just this minute, I received this months issue, which contained the headline / abstract; SIX OUT OF SEVEN US-RUSSIAN "HOTLINES" WILL NOT SURVIVE Y2K. Worried (or just interested) I followed the link and found; Six Out of Seven US-Russian Telephone "Hot Lines" Will Survive Y2K.

Note the clever insertion of 'not' into the first version. So, do we have a 14% or an 85% chance of an unfortunate mis-understanding? Do the operators at the end of those hotlines suffer with the same mis-reading condition? 'Hello Russia, we are [not] really shooting at you'

[The original story came from DNWire and talks about a US Congressional Y2K

committee]

Simon Hogg

🔥 Internet Explorer 5.0 flaws

"Steve Wildstrom" <steve_wildstrom@businessweek.com>

Thu, 30 Sep 1999 21:05:54 -0400

Followers of Microsoft security bulletins have noticed pattern lately: A security hole in Internet Explorer is announced together with a workaround, followed by a patch, followed by a new hole, the workaround, etc.

In fact, all of these holes are part of a much larger problem, one that Microsoft doesn't seem to know how to fix. The difficulty, no surprise here to RISKS readers, lies in ActiveX and its interaction with the browser. ActiveX controls can be marked "safe for scripting," meaning that a script on any HTML page can activate them without requesting permission or giving notification. And the controls turn out to have holes. So far, Microsoft has identified two buffer overruns and one case of improper filesystem access among Microsoft-supplied, marked-safe controls (Security Bulletins MS0099-33, 37, and 40).

But the risks are a great deal worse than that. Anyone, it turns out, can write an ActiveX control and mark it safe for scripting. There's no validation and no enforceable rules. So it's not hard to imagine MyTrojans.com putting a really nasty control on a Web site. The only thing then standing between the user and disaster is Microsoft's flimsy requirement that controls be signed. Most users, confronted by an official-looking certificate, will just click OK, no matter who

has signed
it. Or a nasty control could be signed with a hijacked
certificate.

For now, Microsoft recommends turning off ActiveScripting.
Unfortunately, that breaks a good many Web sites, including most
of
Microsoft's. A less draconian solution suggested to me by a
Microsoft
developer is to deny permission to run "safe for scripting"
controls. But
even this breaks a lot of sites, including Windows Update, which
is most
Windows 98 users' best hope of installing security patches.
Fortunately,
there don't appear to have been any Trojan control exploits yet.

Steve Wildstrom <steve_wildstrom@businessweek.com> Technology &
You,
Business Week 1200 G St NW Suite 1100 202-383-2203 Fax: 202-
383-2125

⚡ Elliptic curve 97-bit challenge broken

Dorothy Denning <denning@cs.georgetown.edu>
Tue, 28 Sep 1999 15:44:17 -0400

[Courtesy of David Farber <farber@cis.upenn.edu>'s IP
distribution]

<http://www.inria.fr/Actualites/pre55-eng.html>

INRIA leads nearly 200 international scientists in cracking code
following
challenge by Canadian company Certicom

Paris, September 28. 1999 - A new code-cracking challenge set
by Certicom
has been successfully overcome using 740 computers in 20
countries over a

period of 40 days. The code, ECC2-97, is based on a technique known as elliptic curves.

Led by Robert Harley, a member of the Cristal project at INRIA, France's National Institute for Research in Computer Science and Control, the 195 researchers involved showed that a 97-bit encryption system based on elliptic curves is more difficult to crack than a 512-bit system based on integers such as RSA-155.

Encryption systems based on elliptic curves have been known since the mid-1980s, but have only recently been adopted by leading encryption companies such as RSA Security Inc. Certicom issued its "ECC Challenge" in November 1997, specifying a series of challenges of increasing difficulty.

The company offers prizes up to US\$100,000. The aim of the challenge is to encourage research in the field of elliptic curves and their applications in encryption, and to strengthen arguments in favor of using elliptic curve cryptography instead of systems based on integer factorization.

The challenge dubbed "ECC2-97" took place in a set of about 10^{29} points on an elliptic curve chosen by Certicom. To solve the problem, participants first computed 119,248,522,782,547 (more than 10^{14}) using open-source software developed by Harley. Among these points, they screened 127,492 "distinctive" points and collected them on a Alpha Linux workstation at INRIA where further processing revealed two twin points. Finally Harley computed the solution using information associated with these

two points,
thus nailing the problem.

The solution was found after less than one third of the predicted computation. The probability of finding the answer so quickly was less than one in ten. Two other twins were detected a few hours after the first - a less than one in 100 probability! Nevertheless the computing power used, around 16,000 MIPS/years, was twice as much as that used for the factorization of RSA-155 announced by Herman Te Riele of CWI (Amsterdam) and his colleagues on 26 August 1999.

"These results strengthen our confidence in codes based on properly-chosen elliptic curves," said Harley. "This needs to be taken into account in standards for security and confidentiality on the Internet."

According to Andrew Odlyzko, Head of Mathematics and Cryptography Research, at AT&T Labs, the code-cracking operation was "a great achievement that demonstrates the value of fruitfully harnessing some of the huge computational power of the Internet that is idle most of the time". He added: "It validates theoretical security predictions, and demonstrates the need to keep increasing cryptographic key sizes to protect against growing threats."

Arjen K. Lenstra, Vice President at Citibanks's Corporate Technology Office in New York and one of the main contributors to the recent successful attack on the RSA-155 challenge, compared the two computational efforts and noted that the present result makes 160-bit ECC keys look even better compared to 1024-bit RSA keys, from a security point of view. "Ideally we

would like
new theoretical advances to further reinforce these practical
results,
although such advances appear out of reach for the moment."

Out of the \$5000 prize money, the team members will give \$4,000
to the Free
Software Foundation to encourage the creation of new free
software. The
remaining \$1,000 go to the team members who identified the twin
points.

Both were in fact found by Paul Bourke using a network of Alpha
workstations, mainly used for studying pulsars at the Centre of
Astrophysics
at Swinburne University in Australia.

The most active teams in the project were:

Astrophysics & Supercomputing,	Australia
INRIA,	France
University of New South Wales,	Australia
"Friends of Rohit Khare",	USA and France
Ecole Polytechnique,	France
Compaq,	USA and Italy
Technischen Universitaet Wien,	Austria
University of Vermont,	USA
"WinTeam",	International
British Telecom Labs,	UK
Internet Security Systems,	UK
Rupture Dot Net,	USA
"Jabberwocky",	USA
Ecole Normale Superieure de Paris,	France

For a complete list of participants consult the project's Web
pages.

Further information:

The ECDL Project: <http://cristal.inria.fr/~harley/ecdl/>

The Certicom ECC Challenge: <http://www.certicom.com/chal/>

Technical contact: Robert Harley, INRIA :
33 1 39 63 51 57 - Robert.Harley@inria.fr

Media contacts: Christine Genest, INRIA :
33 1 39 63 55 18 - Christine.Genest@inria.fr
Sylvie Baranger, Andrew Lloyd & Associates :
33 1 43 22 79 56 - sylvie@ala.com

[Added note from Seth David Schoen <schoen@loyalty.org> in
Dave Farber's IP:

Actually, they did not "show" this in the most important
sense, which is
the mathematical sense. They showed that, using generally
available
techniques, they found it more difficult; they did not show
that the
problem is inherently more difficult. [...]]

⚡ Intuit "Shuts Down" Privacy Site After PRIVACY Forum Query

Lauren Weinstein; PRIVACY Forum Moderator <lauren@vortex.com>

Sat, 25 Sep 99 12:04 PDT

Greetings. An alert PRIVACY Forum reader recently brought a
somewhat
bizarre and certainly ironic situation to my attention. Intuit
(makers of
"Quicken" and other extremely widely-used financial software
packages) had a
web site (<http://privacy.intuit.com>) that presented various
information
regarding their privacy policies.

It also included a feature which allowed any registered Intuit
customer to
view and alter their "privacy preferences." This included data
such as
whether or not they wished to receive promotional materials from
Intuit, how
they should or should not be contacted (e.g. e-mail, phone,
etc.), and
whether or not their name and address would be released to

outside firms.

To access this feature, the customer needed to supply their last name, zip code, and ... *nothing else*! Upon entering any last name and zip code (and given the number of Intuit customers, a hit would be pretty likely for most common names) the user would see the associated first name, city, and last four digits of phone number for that person. The user could then freely modify the privacy preferences for that customer.

Needless to say, I immediately expressed my concern over this situation to Intuit officials. Within a few days, I was contacted by their VP Corporate Communications, informing me that the preference access features of the site had been shut down, and that any users attempting to access them would be directed to an 800 number. A live customer service representative would then verify their contact information before performing any preferences changes. Intuit plans to restore the web preferences feature to the site after making security enhancements, probably within a month or two.

That Intuit responded promptly to my concerns by closing down the feature is to be commended. One must still wonder, however, about the chain of events and review which permitted such an obviously flawed feature to have been implemented in the first place--it is, unfortunately, an all too common sort of situation.

Lauren Weinstein <lauren@vortex.com>, Moderator, PRIVACY Forum; Member, ACM Committee on Computers and Public Policy; Host, "Vortex Reality

Report &
Unreality Trivia Quiz" <http://www.vortex.com/reality>

From PRIVACY Forum Digest Saturday, 25 September 1999 Volume
08 : Issue 13

(<http://www.vortex.com/privacy/priv.08.13>)

Moderated by Lauren Weinstein (lauren@vortex.com)

Vortex Technology, Woodland Hills, CA, U.S.A.

<http://www.vortex.com>

Subscriptions are via an automatic list server system; for
subscription
information, please send a message consisting of the word
"help" (quotes not
included) in the BODY of a message to: "privacy-request@vortex.
com".
Mailing list problems should be reported to "list-maint@vortex.
com".

✶ Henry Petroski, books, and risks of technology

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

Wed, 29 Sep 99 19:51:20 PDT

In the most recent issue of *The New Yorker*, 4 Oct 1999, John
Updike
reviews the latest book by Henry Petroski, someone who has been
mentioned in
many previous issues of RISKS (e.g., 3.25, 9.15-16, 12.51,
18.61). The
newest book is indeed a metabook, ``The Book on the
Bookshelf'' (Knopf,
\$26), a book about books and how they evolved. Updike's review
concludes
with some of the risks of books using computer technology as the
medium
itself, the constraints of reading from CD-ROMs, the effects of
hackers and
electromagnetic catastrophes on the computer forms, the gradual

ebbing away
of seldom-read books into computer warehouses, and the MIT
Overbook. Both
Petroski's book and Updike's review make fascinating reading.

⚡ Linux banned after Samba misconfiguration blocks NT authentication

"B. W. Fitzpatrick" <fitz@red-bean.com>
Fri, 01 Oct 1999 00:04:09 -0500

I received this from a friend who works at A Very Large Corporation and has requested that both he and the company remain anonymous. From what I can tell, someone at said company was fiddling with a Linux box and configured it to be the Primary Domain Controller (instead of authenticating off of the Primary Domain Controller). Well, this hosed all NT domain authentication in the company and prevented anyone from authenticating until the offending PDC was removed from the network. The end result? The company is banning Linux.

Now, this **exact** same thing happened to a friend of mine at another company, but it was quickly fixed, identified, and Linux is still in use there today. Same problem, different result.

While I'm not by any means an NT guru, this seems to be a HUGE vulnerability in the NT Domain Authentication mechanism--if I ran a network where anyone can plug into my network and stop all authentication this easily, I would be scared out of my wits.

Here's the body of the e-mail. I for one would like to send the author a

copy of "On Writing Well." The names have been changed to protect the ignorant:

We have encountered an incident with the Linux desktop operating system. A Linux box named <foobar> had assumed control of our domain yesterday and temporarily paralyzed our network. The box has been identified and shut down. Affective[sic] immediately, all use of Linux systems within the <company name> domain will be discontinued until further notice.

We will need to justify Linux opportunities within <company name> followed by a thorough evaluation of the ramifications of deploying this new technology. Along with the identification of security risks, policy must also be established to properly administer Linux within our environment.

All cooperation with this notice is required and appreciated. We will define a focus group to address this challenge. If anyone wishes to be part of this study, please feel free to let me know. I'll keep you all apprised of our status.

The RISK? Attacking the symptoms and not the problem doesn't really solve anything.

Brian W. Fitzpatrick, Project Manager/Lead Programmer

Cyber-Speak

Ira J Rimson <irimson@compuserve.com>

Tue, 28 Sep 1999 15:27:11 -0400

Maybe some of you can explain the logic behind the following note received

from my UK friend Jonathan Berman:

We've just bought a new colour printer for the office.

The instructions included the following important message:

"Note: The Starter CD includes a utility to easily copy the HP Deskjet

1120C printer software to 3.5-inch, high-density diskettes. This allows

you to use the diskettes to install the software on systems that do not

have a CD-ROM drive. See the Printer Software menu in the Starter CD"

Am I missing something obvious here?



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 62

Tuesday 12 October 1999

Contents

- [Serious security flaw in Microsoft Java](#)
[Edward W. Felten](#)
- [Latest British train collision](#)
[PGN](#)
- [TCAS unit flaw](#)
[Steve Bellovin](#)
- [Glitch switches Nevada 911 calls to San Diego CHP](#)
[Carl Maniscalco](#)
- [Supercomputer lost to fire, weather predictions reduced](#)
[Andrew Klossner](#)
- [Calif government computers fail, cars impounded, ...](#)
[Declan McCullagh](#)
- [Re: Massive fiber cut](#)
[Doneel Edelson](#)
- [ICD's save ISS: *not*!](#)
[Erann Gat](#)
- [Floyd/EDS](#)
[William Addams Reitwiesner](#)
- [Re: Internet Explorer 5.0 flaws](#)
[Dan Wallach](#)

- [GPS rollover *did* cause DoD Problems](#)
[Peter B. Ladkin](#)
 - [NT Stung Again by Y2K Bug](#)
[Paul Walczak](#)
 - [Iraq decides to wait and see on Y2K oil disruption](#)
[Keith A Rhodes](#)
 - [FBI warns some Y2K fixes may be suspect](#)
[Jonathan de Boyne Pollard](#)
 - ["Self-destructing e-mail"](#)
[Brad Arkin](#)
 - [Re: Linux banned](#)
[Mark Brader](#)
 - [Where do you want to be *mis*directed today?](#)
[Mark Brader](#)
 - [Maybe Microsoft owns stock in Canada?](#)
[Mark Brader](#)
 - [Risks of screen saver messages](#)
[Nick Brown](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Serious security flaw in Microsoft Java**

"Edward W. Felten" <felten@cs.princeton.edu>

Tue, 12 Oct 1999 16:29:03 -0400

Karsten Sohr at the University of Marburg has discovered another serious security flaw in Microsoft's Java Virtual Machine. A bug in Microsoft's bytecode verifier allows the construction of code sequences that illegally cast values of one Java type to values of another unrelated type, in violation of Java's typing rules, without detection by Microsoft's verifier. A malicious applet can exploit this flaw to breach the JVM's security, and

can then proceed to do anything it wants to do on the victim's computer.

For example, a malicious applet might exploit this flaw to read private data, modify or delete files, or eavesdrop on the user's activities.

Dirk Balfanz and I, at Princeton University, have constructed a demonstration applet that exploits this flaw to delete a file.

All recent versions of Microsoft's JVM for Windows appear to be vulnerable, so users of recent versions of Internet Explorer are affected by this flaw.

A malicious applet could also be embedded in an e-mail message read using Microsoft Outlook or Eudora. Users of other JVMs, browsers, and email readers are generally not affected. (Thanks to Reliable Software Technologies for their help in testing on various platforms.)

We have reported this flaw to Microsoft and they are working to address it.

For more information, contact Karsten Sohr (sohr@mathematik.uni-marburg.de) or Edward Felten (felten@cs.princeton.edu, phone (609) 258-5906).

Edward Felten, Secure Internet Programming Lab, Dept. of Computer Science
Princeton University

Latest British train collision

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

Sun, 10 Oct 99 12:16:57 PDT

The latest head-on collision occurred at the same Signal 109 near Ladbroke

Grove in Western London as the collision that occurred two years

ago (almost to the day). The previous accident occurred when one driver was looking downward and somehow missed two Red signals. The latest accident was also attributed to a driver missing a Red signal, this time the driver of a commuter train that crashed with a high-speed intercity train from Cheltenham. The train had an Automatic Train Protection System, but it was switched off because it was ``not operational''. Its operation might have helped, although it reportedly would not by itself have prevented the accident. A new Train Protection Warning System had been scheduled to be installed at Signal 109 in December 2003, along with many other places.

[Source: *The New York Times*, 9 Oct 1999, which noted at least 70 deaths and 64 people unaccounted for.]

[Owen Hopkins noted that 8 trains have run past this signal in the past

6 years. Signal 63 has an even worse record. Comments also from

Jonathan Pritchard... With the breaking up of British Rail, there is no

one organization left to rail at? PGN]

[CORRECTION: My statement that the previous accident involved the

same signal is INCORRECT. It will be corrected in the next issue. PGN]

[Second correction: The number of deaths was incorrectly reported.

See [RISKS-20.68](#). PGN]

TCAS unit flaw

Steve Bellovin <smb@research.att.com>

Tue, 12 Oct 1999 10:00:40 -0400

There's a fascinating article in the 12 Oct 1999 **Wall Street Journal** about how a flaw in a TCAS (Traffic Alert and Collision Avoidance System) nearly caused a crash, rather than preventing one.

On 28 Jun 1999, a British Airways jet and a Korean Air jet nearly collided when the latter's TCAS unit told the pilot to climb. The Korean Air plane was 2000 feet below the British Airways plane; however, the pilot was told that it was in fact 400 feet **above** it. That's too close, so the pilot was advised to climb. And that, of course, almost induced a collision.

Part of the problem was with a circuit that sends the plane's altitude to the TCAS system and to the transponder. The circuit uses an 11-bit code over a parallel connection; a single-bit error, which occurred in testing, would correspond to a 2400 foot difference in altitude -- precisely the error here. (The article also notes that on a previous flight, the crew of this plane was advised that their transponder was giving the wrong altitude.)

The British Airways jet, though, had a TCAS system that noticed an instantaneous jump in the altitude of the other plane. Since that's impossible, the bad readings were properly ignored, which in turn meant that there was no warning to the crew. When the TCAS system finally

did detect
that the other plane was climbing towards it, it could only say
tell the
pilots to dive, since the other plane was climbing. But that,
according to
the article, was precisely the wrong thing to do.

The Korean Airways jet's TCAS system does include a comparator
circuit to
verify the altitude reading. Due to a wiring problem, however,
that circuit
was silently disabled; there is no warning to either pilots or
mechanics of
this condition. And the faulty altitude reading occurred when
engineers
left the air-data computer "on for a long time and added extra
electrical
power".

The article closes by noting that the only thing that saved the
two planes
was marginally inaccurate navigation, and that if GPS-based
systems were in
use, the planes would have collided head-on.

✶ Glitch switches Nevada 911 calls to San Diego CHP

Carl Maniscalco <caman@earthlink.net>

Thu, 7 Oct 1999 14:40:09 -0800

On the afternoon of 30 Sep 1999 and continuing to the next day,
dispatchers
at the California Highway Patrol's San Diego communication
center started
receiving cellular 911 calls from Nevada, with callers reporting
accidents
at local Nevada street name unfamiliar to the dispatchers. When
they
finally figured out what was happening, calls were transferred

back to the

Nevada Highway Patrol for redistribution an appropriate dispatcher.

Apparently, the problem was at the Nevada switching center for Sprint PCS

and Pacific Bell. [Source: *San Diego Union-Tribune*, 2 Oct 1999, PGN-ed]

⚡ Supercomputer lost to fire, weather predictions reduced

Andrew Klossner <andrew@pogo.WV.TEK.COM>

Thu, 07 Oct 1999 10:10:19 -0700

The U.S. National Centers for Environmental Prediction (NCEP) lost their

Cray C90 supercomputer in a fire, as reported in

<http://www.ncep.noaa.gov/director/supercomputer/>

Weather prediction runs have moved to slower backup machines.

They are not

being run as often and are not looking as far in the future.

"There is no

objective basis for making forecasts at the 8-14 day range, and no further

messages of forecasts will be issued until model guidance at that range

again becomes available."

Andrew Klossner (andrew@pogo.wv.tek.com)

⚡ Calif government computers fail, cars impounded, ...

Declan McCullagh <declan@well.com>

Mon, 04 Oct 1999 15:59:03 -0400

Massive computer crashes have repeatedly forced California agencies to turn away customers for driver's licenses, food vouchers and other services. The Highway Patrol suddenly had difficulty checking criminal records. Child Protective Services could not get quick access to abuse files. For two days Glendale's DMV office had to process driver's license renewals manually. And one consulting firm clocked 19,000 minutes of intermittent outages in the first half of 1999. Some cars were impounded because computer records incorrectly showed licenses had expired. The Women, Infants and Children program reported a severe drop in participation, and had to return \$5.7 million in unspent Federal funds. There were lots of long lines. [Source: PacBell Blamed for Failures of State Computers By VIRGINIA ELLIS, *Los Angeles Times*, 4 Oct 1999 <http://www.latimes.com/HOME/NEWS/STATE/topstory.html>; PGN-ed]

✶ Re: Massive fiber cut (Farber, [RISKS-20.61](#))

"Edelson, Doneel" <doneeledelson@aciins.com>

Thu, 7 Oct 1999 17:03:22 -0400

The fiber-optic cable cut by a gas-company employee 30 miles east of Cleveland, Ohio, disrupted Internet traffic nationwide for almost 12 hours on 29 Sep 1999. On the good side, here is a quote from *PCWeek*: ``As bad as it was, [Vaughan] Harring [a spokesman for GTE Internetworking] said it might have been worse without the redundancies most ISPs have

built into
their networks. "This was a significant cut. If something of
this size
happened a year ago, it would be more than degraded service....
We'd be
talking about a hard outage." ''
[<<http://www.zdnet.com/pcweek/stories/news/0,4153,1017468,00.html>>, PGN-ed.]

⚡ ICD's save ISS: *not*!

Erann Gat <gat@binkley.jpl.nasa.gov>
Wed, 6 Oct 1999 11:30:02 -0700 (PDT)

>From http://www.space.com/news/spacestation/iss_metric_991005.html

Space Station Immune to Metric Mishap, NASA Says
By Daniel Sorid, 05 Oct 1999

The International Space Station will not fall victim to the
measurement
units problems which ruined the Mars Climate Orbiter,
according to a NASA
spokesman. In the early 90s, engineers put together a so-
called interface
control document, which identifies the use of metric or
English units for
every piece in the station, according to NASA spokesman Dwayne
Brown.
"This is not a new issue for us," Brown said. "It's so well
documented
that we don't have that problem." The document also shows
where metric
and non-metric units interact with each other, and calls for
the
development of adapters that standardize the units.
"Engineers got
together and said, 'Here's the piece of hardware. Let's see

where they

interconnect.' If we've got a metric piece and an English piece, that

will show up very clearly in the document." [...]

There's one little problem with this theory: Mars Climate Orbiter had an

interface control document too. (JPL is ISO9000 certified! We have

documents for everything.) It was obviously not enough to save MCO; why

should it be any different for ISS?

Most accounts in the press make the MCO disaster sound like a massive

breakdown in communications, with one group of people doing everything in

Metric and another doing everything in English units, and no one talking to

anyone else for months on end. I was told this morning by a member of the

MCO team that this is not true. Everyone knew that everything was supposed

to be Metric across the board. The problem was a single number in the

software that was accidentally entered incorrectly. The exact same thing

has happened on at least one previous mission, but the problem was caught

before it became a news story (that is, before we drove the spacecraft into

a planet.)

Regular readers of RISKS will no doubt be shocked -- shocked! -- by these

revelations.

Erann Gat <gat@jpl.nasa.gov> [Usual disclaimers]

 **Floyd/EDS**

William Addams Reitwiesner <wrei@erols.com>

Tue, 5 Oct 1999 21:53:57 -0400 (EDT)

At the Library of Congress, where I work, the ATM network for the LC Credit Union was down for most of a week, with typed fliers pasted to the ATMs blaming the outage on Floyd-related flooding in New Jersey, and saying that we were one of a number of institutions which were affected by this. I was mildly surprised to see nothing about this in RISKS, but I found the following in a Y2K Usenet newsgroup (version below lifted from www.deja.com):

```
>         >> Forum: comp.software.year-2000
>         >> Thread: Detailed reports on Floyd-EDS glitch
>         >> Message 8 of 9
>
> Subject: Detailed reports on Floyd-EDS glitch
> Date: 1999/09/27
> Author: John Denver <jd@howdyfolks.org>
>   Posting History Post Reply
>
> The following articles were found in the Bergen County
Record. Glen
>   Rock, NJ is located in Bergen County.
>
>   (9/23/99) Floyd struck a hub linking 23 centers
>
>   From the article:
>   "Banks whose data lines fed into the local phone system via
the
>   Rochelle Park hub lost their ATMs. A large facility down the
street
>   owned by Electronic Data Systems Corp. also flooded,
disrupting
>   service to their network of 8,000 ATMs across the country.
Those
>   troubles were largely unrelated to the phone company's
problems."
```

>
> Also, see:
> (9/26/99)Dress rehearsal for Y2K distress: Can millennium
match Floyd?
> <http://www.bergen.com/news/ytkrg199909262.htm>
>
> Apparently, hearings are being conducted today (9/27) on this
> fictitious unconfirmed problem:
> "These questions could be raised in regulatory proceedings
against the
> company, as well as at a meeting Monday involving phone
company
> officials and U.S. Sen. Frank R. Lautenberg, D-N.J., and U.
S. Reps.
> Steve Rothman, D-Fair Lawn; Marge Roukema, R-Ridgewood, and
Bill
> Pascrell Jr., D-Paterson."
>
> Oh yeah, and a search for "Rochelle Park" at EDS.com
yields... nothing.

[I noted in [RISKS-20.58](#) that my Maryland course on survivable
systems

had survivability problems in the second and third lectures
(lightning and

Floyd, respectively. Here is an update. For the fourth
lecture (I was at

SRI), the students in the classroom had intermittent video
failures,

attributed to ISDN lines still being flaky after the
hurricane. For the

fifth lecture, the classroom had audio only. The problem was
eventually

traced to the aftermath of the lightning strike three weeks
earlier: the

PC reboot had not included some updates for the video
configuration.

Mercifully, the sixth lecture was uneventful. So, only two of
the six

lectures failed to exhibit self-referential survivability
problems. PGN]

⚡ Re: Internet Explorer 5.0 flaws ([Risks 20.61](#))

Dan Wallach <dwallach@cs.rice.edu>

Tue, 05 Oct 1999 22:44:02 -0500

Steve Wildstrom points out (in [Risks 20.61](#)), that ActiveX has been a thorn in Microsoft's side, which is certainly true. He seems to suggest, however, that **all** of Microsoft's problems boil down to problems in ActiveX, which is **not** true.

Together with colleagues at Princeton and Xerox PARC, we recently found a bug in Microsoft's Java VM (see [Risks 20.55](#)) that would let an attacker compromise the VM, irrespective of the target's ActiveX settings. Historically, it seems bugs have been found throughout Microsoft's systems, ranging from TCP/IP fragment reassembly (e.g., "the ping of death") through Microsoft's Web services, such as the recent HotMail privacy incident.

While I would certainly enjoy seeing Microsoft reinvent their ActiveX architecture in favor of something that provided reasonable security guarantees (and, heaven forbid, portability across operating systems), that would only be the first step on the road ahead for Microsoft.

Dan Wallach, Rice University

⚡ GPS rollover **did** cause DoD Problems

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Fri, 08 Oct 1999 16:11:47 +0200

Mike Martin reported on the problems with Tokyo taxicabs caused by the August GPS rollover ([Risks-20.55](#)). Aviation Week reports (Oct 4, p32) that US DoD systems also had problems with weapons systems, even though the situation had been anticipated. "...the fault lay in the way the Pentagon's two primary mission planning systems, the Air Force Mission Support System (AFMSS) and the Navy's Tactical Aircraft Mission Planning System, were providing the data to weapons systems."

The mission planning tools provide, amongst other things, the approximate location of the GPS satellites to a weapons system GPS receiver so that the receiver can avoid large-sweep searching for the satellites. Some receivers work with 16-bit week data; the satellites and mission planners rolled over; and the different formats caused "conflicting data sets" and thus problems, according to AvWeek.

"Short-term fixes...include editing the missions planning data manually, having the receivers find the satellites unaided or downloading the almanac data directly from the satellite, which takes about 13 min.

The likely long-term fix is a software modification to AFMSS and TAMPS, which is considered cheaper than modifying weapons systems hardware."

Peter Ladkin <http://www.rvs.uni-bielefeld.de>
University of Bielefeld, Germany

⚡ NT Stung Again by Y2K Bug

<pwalczak@mail.arl.mil>

Thu, 30 Sep 1999 21:39:37 -0400

Microsoft's May 1999 Service Pack 5 (SP5) was supposed make Windows NT 4.0 ready for Y2K. However, so many bugs arose that fixes have been included in SP6, which has been in beta since July. There are problems with the Net User command line security utility for setting log-in times, with real-time clock dates when not in a daylight-saving time zone, and with multiprocessor kernels, another problem with Outlook Express, etc. The problems are considered minor. Problems with other systems are also noted. [Source: NT Stung Again by Y2K Bug, Joseph McKendrick, 22 Sep 1999 <<http://www.entmag.com/displayarticle.asp?ID=9239933447PM>>, PGN-ed]

⚡ Iraq decides to wait and see on Y2K oil disruption

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

Fri, 01 Oct 1999 11:21:49 -0400

[Keith sent in a Reuters item noting that Iraq is has decided to avoid the costs of Y2K upgrades, and may have to shut down production for the new year instead. Many of their computers are reportedly old process controllers. Keith comments that with Iraq and Venezuela both lagging in Y2K fixes, it could be an expensive millennium for many drivers. PGN-ed]

✶ FBI warns some Y2K fixes may be suspect ([RISKS-20.61](#))

Jonathan de Boyne Pollard <J.deBoynePollard@tesco.net>

Wed, 06 Oct 1999 11:19:55 +0100

> The Federal Bureau of Investigation says that some of the
> Y2K-related programming fixes that were undertaken by
> foreign contractors may contain malicious code. [...]
> Such code could contain "time bombs" set to detonate at
> some future date, [...]

And how, exactly, would that be any different from the code that
was there
before ? (-:

JdeBP

✶ "Self-destructing e-mail"

Brad Arkin <barkin@rstcorp.com>

Fri, 08 Oct 1999 09:25:52 -0400

Intrigued by the headline "'Self-destruct' e-mail offers virtual
privacy"

(<http://www.usatoday.com/life/cyber/tech/review/crg441.htm>), I

did some more

investigating. Disappearing Inc. (<http://www.disappearing.com/>)

has few

technical details on its web site, but the general idea is that
by using

their plug-in two people can send and receive encrypted messages
with the

added feature that the key is held by Disappearing Inc. Anytime
the

recipient wishes to read the message, they must authenticate
themselves to

Disappearing Inc. in order to retrieve the key. Disappearing Inc. logs all accesses to the key and destroys the key at the end of its life span.

Disappearing Inc. claims that once the key is destroyed the message can never be read again, and thus the message has effectively self-destructed like a Mission:Impossible assignment.

While it is possible (although sadly, unlikely) that Disappearing Inc. has implemented this system using an appropriate mix of good authentication scheme, strong encryption algorithm, secure key generation, high level of site security, and secure key transmission it doesn't really matter. All Disappearing Inc. offers is a variant of third party key escrow and nothing more. The problems with key escrow have been well documented.

By forcing users to go across the network to retrieve a key (which may have already expired) every time they want to read a locally stored message, it is a certainty that users will instead simply cut and paste any message worth reading again into a plaintext file outside the control of Disappearing Inc.'s encryption. The potential problems with this scheme are too many to list here, and my opinion is that users should cut out the middle man and use a package like PGP instead.

Brad Arkin, Software Security Group Reliable Software Technologies

✶ Re: Linux banned (Fitzpatrick, [RISKS-20.61](#))

Mark Brader <msbrader@interlog.com>

Mon, 4 Oct 99 8:43:48 PDT

By the way, Brian Fitzpatrick's item in [RISKS-20.61](#) about Linux being banned from a company for silly reasons reminds me of another anecdote in Feynman's books. From memory:

Filing cabinets at Los Alamos were provided with combination locks, but these were seriously flawed; a person who had physical access to the cabinet while it was open could subsequently discover the combination and open it in a few minutes. Feynman identified this security risk and informed the people in charge... who responded by ordering all people with such cabinets *that Feynman had had physical access to* to change their combinations!

🔥 Where do you want to be *mis*directed today?

<msbrader@interlog.com>

Fri, 1 Oct 1999 00:52:38 -0400 (EDT)

[Erwin Mascardo <mascardo@admin.assuren.net> posted the following to rec.humor.funny. (It's in their archive at <http://www.netfunny.com/rhf/jokes/99/Sep/expedia.html>.)]

My wife recently went on a business trip, and in filling out her expense report, she noted that she could claim the mileage to and from the airport. My first attempt at using MapQuest to calculate the distance failed, so I tried Microsoft Expedia Maps. After the shock wore off, my only

regret was that my wife couldn't really claim this mileage figure, as we had no way to prove that we'd spent 9 days driving to Newfoundland and back. Highlights from the Microsoft-generated directions follow:

Summary

>From: Laurel, Maryland
To: Baltimore-Washington International Airport, Maryland
Driving Distance: 5865.1 miles
Time: 9 day(s) 3 hour(s) 22 minute(s)

Driving Directions

Time	Instruction
0:00	Depart Laurel, Maryland
1:01	Entering Delaware
1:17	Entering New Jersey
3:24	Entering New York
3:51	Entering Connecticut
5:51	Entering Massachusetts
7:29	Entering New Hampshire
7:44	Entering Maine
12:20	Entering New Brunswick
20:20	Take the North Sydney-Argentia Ferry
34:32	Entering Newfoundland
36:35	Turn left onto Local road(s) (4543.1 mi)
219:22	Arrive Baltimore-Washington International Airport, Maryland

I guess when Microsoft asks "Where do you want to go today?" that *how* you get there isn't always important...

(A subsequent attempt at MapQuest gave the correct figure of 16.5 miles.)

[Forwarded to Risks by Mark Brader]

⚡ Maybe Microsoft owns stock in Canada?

<msbrader@interlog.com>

Fri, 1 Oct 1999 01:01:24 -0400 (EDT)

This one was posted to rec.humor.d, the followups-to-jokes group, by Bill

Seurer <BillSeurer@vnet.ibm.com>. Some misformatting in his posting is

fixed in this copy. --Mark Brader]

X-no-archive: yes

Erwin's wife wasn't the only one to get misdirected. I wonder if Microsoft owns that North Sydney-Argentia Ferry?

Here is the trip Expedia proposed for a brother of one of my buddies. I left off the compass directions and mileage parts. Do note that 14 hour ferry ride, too!

Summary

> From: Hastings, Minnesota
> To: Saint Charles [St. Charles], Minnesota
> Driving Distance: 6758.6 miles
> Time: 9 day(s) 17 hour(s) 30 minute(s)

Driving Directions

Time	Instruction
0:00	Depart Hastings, Minnesota
0:03	Entering Wisconsin
1:47	At I-94 Exit 88, turn right onto I-94
2:41	Go onto I-90
4:51	Entering Illinois
6:40	Entering Indiana
7:01	At I-80 Exit 16, bear left onto I-94
7:29	Entering Michigan
10:42	At I-94 Exit 204A, turn right onto SR-39
10:46	At I-75 Exit 41, turn left onto I-75
10:55	At I-75 Exit 47, turn right onto SR-3
10:56	Turn right onto W Grand Blvd
10:57	Entering Ontario

10:57	Bear left onto S-3
11:04	Turn left onto S-2
11:06	Bear right onto S-3B
11:08	Bear left onto S-401
18:50	Entering Québec
18:50	Go onto C20
19:31	Bear left onto C720
19:37	Turn right onto S-134
19:40	At Longueuil, turn left onto C20
23:39	Bear right onto TC-185
24:39	Entering New Brunswick
24:41	Bear left onto TC-2
28:10	Go onto S-695
28:20	Turn left onto S-710
28:31	Turn left onto TC-2
28:35	Turn right onto S-112
29:17	At Salisbury, turn left onto S-106
29:46	Bear right onto TC-2
30:04	Entering Nova Scotia
30:06	Turn right onto TC-104
30:51	At Wentworth Centre, turn left onto S-246
31:02	Bear right onto S-256
31:42	Turn right onto S-6
31:44	At Pictou, bear right onto TC-106
31:50	Go onto TC-104
32:03	Bear right onto S-4
32:05	Go onto TC-104
32:08	Go onto S-4
32:14	Bear left onto TC-104
32:19	Bear left onto S-4
32:28	Bear left onto TC-104
33:01	At Mulgrave [Port Mulgrave], go onto TC-105
34:23	At Sydney Mines [Sidney Mines], bear left
onto S-223	
34:27	At North Sydney, turn left onto Local road(s)
34:29	Take the North Sydney-Argentia Ferry *CHECK
TIMETABLE*	
48:40	Take the Local road(s)
48:41	Entering Newfoundland
48:44	At Freshwater, go onto S-100
49:14	Bear right onto TC-1
49:41	Bear right onto S-13
49:54	At Bay Bulls, turn right onto S-10

50:43 Turn left onto Local road(s) (SE 4543.1
miles)

233:30 Arrive Saint Charles [St. Charles],
Minnesota

Bill Seurer, Compiler Development, IBM Rochester, MN
Bill_Seurer AT us.ibm.com Bill AT seurer.net <http://www.seurer.net/>

⚡ Risks of screen saver messages

BROWN Nick <Nick.BROWN@coe.int>

Wed, 6 Oct 1999 12:44:53 +0200

France Info radio reported today (1999-10-06) that an investigation into police racism has been started in a small French town after a citizen, visiting the police station, observed a slogan with racist overtones scrolling across the screen of a PC on a desk in the reception area.

The officer responsible for the PC claimed that the reference to "melons" (a French racist term of abuse, but also a legitimate word for the round fruit which has the same name in English) referred to his daughter's passion for harvesting said fruit.

Regardless of the plausibility or otherwise of that statement, the RISK is clear: your screen saver message, scrolling away in bright mauve 24 point type, and quite possibly the only thing moving to catch people's attention, might say more about you than, say, a poster inside your locker ever could...

Nick Brown, Strasbourg, France.

email address updates : @coe.int replaces @coe.fr
for more information, <http://dct.coe.int/info/emfci001.htm>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 63

Saturday 16 October 1999

Contents

- [Rome railway station shutdown](#)
[Peter B. Ladkin](#)
- [Washington DC Metrorail to Replace Relay System](#)
[George Beuselinck](#)
- [Aircraft computer redundancy and airline safety](#)
[Julian Olson](#)
- [Y2K creates "horseless carriages"](#)
[Jim Griffith](#)
- [INS Irony](#)
[Paul Robinson](#)
- [Re: Signal 109 near Ladbroke](#)
[Robert Evans](#)
- [Re: Mars Climate Orbiter units confusion](#)
[Clive Page](#)
- [Extra information in Word documents](#)
[Steven M. Bellovin](#)
- [Cyberwarfare: The Business Opportunity](#)
[Monty Solomon](#)
- [Millennium Bugs?](#)
[Rick Downes](#)

- [You can't get where you want to go today](#)
[J Fieber](#)
 - [Odd synchronicity in items in RISKS-20.62](#)
[Chris Smith](#)
 - [Re: Cyber-Speak](#)
[Martin Minow](#)
 - [Bell Atlantic forgets: exchanges are not unique between area codes](#)
[Jonathan I. Kamens](#)
 - [Yet another case of credit-card 'security'](#)
[E. Lange](#)
 - [CFP: FTCS-30 & DCCA-8 Int'l Conf on Dependable Systems and Networks](#)
[Philip Koopman](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Rome railway station shutdown

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Wed, 13 Oct 1999 18:50:27 +0200

Traffic at Rome's main railway station was disrupted for the fourth day on Tuesday 12th October as trains were rerouted and cancelled due to a malfunctioning new computer system. The station was shut down at the weekend for installation of the new command system and apparently it didn't work properly when passengers arrived Monday. Arrivals have been delayed up to 2 hours and departures by up to 50 minutes (or infinity)

Source: International Herald Tribune, Wednesday Oct 13, p2

Prof. Peter Ladkin Ph.D. <http://www.rvs.uni-bielefeld.de>
University of Bielefeld, Germany

✶ Washington DC Metrorail to Replace Relay System

"George Beuselinck" <gb944@mindspring.com>

Fri, 15 Oct 1999 05:13:04 -0400

The Washington DC Metro has had rampant failures among its electronic relays, and as a result has been running the entire system manually since April 1999. The relays had a life expectancy of 70 years, having been installed in the 1970s, with an expected malfunction rate of one every 50 years. Although the source of the premature aging is still unknown, it has been decided to replace all 20,000 relays with new ones -- which is expected to permit resumption of automatic operation by May 2000. [PGN-ed,

Source: <http://www.washingtonpost.com/wp-srv/local/daily/oct99/metrol5.html>

"In December, a train was told to go 45 mph on a stretch of track with a 15 mph speed limit. In February, a train was directed to travel at 0 mph when it should have been ordered to move at 15 mph. And in March, a train was halted when it got a red, or stop, signal, but the rail ahead was clear, and it should have received a green signal to proceed."

[Typo in 20,000 fixed in archive copy. PGN]

✶ Aircraft computer redundancy and airline safety

"Julian Olson" <jolson@CAM.ORG>

Wed, 13 Oct 1999 11:12:39 -0400 (EDT)

We recently flew from Montreal to Washington by way of Detroit (an interesting way for the deregulated market to deal with our fuel resources).

A few minutes after the scheduled departure time in Detroit, the captain informed us that there would be a delay while a technician was summoned to deal with a malfunctioning computer. After inspection of the situation, it was determined that we would take off as soon as the twenty-minute shutdown procedure had been carried out. "We are allowed", said the captain "to take off even if this backup computer is not working". There was no explanation of why the builder of the aircraft would have gone to the expense of including an unnecessary computer.

This may have been a quite benign situation and the policy entirely reasonable - I am not qualified to judge it - but I couldn't help wondering who did the allowing. It wasn't hard to imagine some bean counter weighing dollars against safety and deciding that such cases should be resolved in favor of expediency.

Since this was an A320, reputed - fairly or not - to depend very heavily, if not excessively, on computers to stay in the air, it didn't encourage a sense of security. I would be grateful for enlightenment from someone who understands the issues.

Julian Olson <jolson@cam.org>

⚡ Y2K creates "horseless carriages"

Jim Griffith <griffith@netcom.com>

Tue, 12 Oct 1999 16:28:44 -0700 (PDT)

AP reports that a Y2K glitch has caused 2000 new vehicle registrations in the state of Maine to bear the classification "horseless carriage".

Apparently, the DMV software misread the 2000 model year as 1900, and it is hardwired to classify any vehicle with a model year before 1916 as a horseless carriage.

<http://www.mercurynews.com/breaking/docs/024281.htm>

⚡ INS Irony

Paul Robinson <rfc1394a@aol.com>

Sat, 16 Oct 1999 09:54:55 EDT

The following item was reported in the UK's Silicon.Com weekly round-up:

The US government admitted this week that it had accidentally issued more visas for foreign high-tech workers than it had intended - 20,000 to be precise. Why? Because of a computer glitch. Irony once again rears its ugly head and slaps the authorities around the face with a wet fish.

✶ Re: Signal 109 near Ladbroke ([RISKS-20.62](#))

Robert Evans <rhe@nosc.ja.net>

Wed, 13 Oct 1999 01:02:18 +0100 (BST)

I'm sure that others have also pointed these out, but there are some errors in the source you used for the information on the train crash.

> The latest head-on collision occurred at the same Signal 109 near Ladbroke
> Grove in Western London as the collision that occurred two years ago (almost
> to the day).

The Ladbroke Grove crash happened on the same line, but some distance away from the Southall crash of two years previously. Signal 109 was not involved in that incident, but has been involved in near-misses recently.

> The train had an Automatic Train Protection System, but it was
> switched off because it was ``not operational''. Its operation might have
> helped, although it reportedly would not by itself have prevented the
> accident.

The Great Western train from Cheltenham did have ATP which was disabled, but it would have made absolutely no difference, as the Great Western train had a green signal. At the very last minute a signal operator has noticed that the Thames commuter service had passed SN109 at danger (red), and changed SN120 to red for the Great Western service, but this was moments before the collision, far too late for even the best braking systems to have made any

difference. The Thames Trains service did not have ATP.

Sources for the above are the BBC News website, the *Independent* newspaper, and many hours of TV coverage (being a regular traveller on the line).

⚡ Re: Mars Climate Orbiter units confusion

Clive Page <cgp@star.le.ac.uk>

Wed, 13 Oct 1999 09:30:21 +0100 (BST)

Observatory magazine (<http://www.ulo.ucl.ac.uk/obsmag/>) reports a NASA press release dated 11 Sep 1998 11 on the Mars Climate Orbiter which originally said:

"It is 7.6 feet (25 metres) high, 6.4 feet (21 metres) deep, and 5.4 feet (18 metres) wide".

This press release (<http://mars.jpl.nasa.gov/msp98/news/news23.html>) is

still on-line but was last edited only a few days ago. Perhaps if this unconventional conversion from Imperial to Metric units had been noticed sooner, the mission might have survived?

Clive Page, Dept of Physics & Astronomy, University of Leicester, Leicester, LE1 7RH, U.K. +44 116 252 3551

⚡ Extra information in Word documents

"Steven M. Bellovin" <smb@research.att.com>

Tue, 12 Oct 1999 15:19:44 -0400

We've seen many stories, over the years, of information leaking via Word documents. Perhaps the most amusing such story is reported in Salon magazine. According to http://www.salon.com/tech/log/1999/10/12/microsoft_report/index.html, Microsoft's annual report was written on a Macintosh computer...

✶ Cyberwarfare: The Business Opportunity

Monty Solomon <monty@roscom.com>
Sat, 9 Oct 1999 00:10:06 -0400

http://www.thestandard.com/articles/mediagrok_display/0,1185,6870,00.html

Cyberwarfare: The Business Opportunity

Grab your digital trench coat - and your business plan. The U.S. has announced that it will enter the cyberspook business in earnest by establishing a new center to combat (and practice) online espionage. On its face, this was not a business story, and outlets played it straight, allowing generals and senators to speak gravely of cyberwarfare. But between the martial drumbeats, a few hints fell to the effect that this initiative could help U.S. businesses in a big way.

✶ Millennium Bugs?

<main@radsoft.net>

Sat, 01 Jan 2000 00:37:14 +0000

It is now finally clear to me what all the hysteria about Y2K is really all about.

It is not about stingy COBOL programmers using two BCD bytes instead of four in WORKING STORAGE.

It is not about embedded systems collapsing, rendering our traffic intersections, our satellite systems, and other vital technologies useless.

It is about the latest in a long debilitating line of systemware products from Redmond, Washington, USA.

This week I received the WinNT Magazine newsletter, with an introduction from Paul Thurrott, who describes himself as a "recovering Windows 2000 (Win2K) beta tester". Thurrott is largely positive about this monster, but does add that hardware requirements "have risen from a lowly Pentium to a 300MHz Pentium II with 128MB of RAM" and winds up by saying:

"But I suspect that when the Win2K beta ends, a lot of testers are going to find themselves balking at the upgrade, at least for the short term. Suddenly, that wonderful ugly duckling we know as NT 4.0 doesn't look so bad after all."

It just dawned on me - namely that the great, great majority of PC users world-wide are home computer enthusiasts, and the great, great

majority of these enthusiasts use their computer primarily - or even exclusively - to access the Internet, and that they demonstrably do not need anywhere near the kind of machine necessary to run Win2K to do that, and that they don't need Win2K at all.

And it dawned on me further that this would hardly change anything. Home computers running 16 bit operating systems might be perfectly capable of rendering an enjoyable cyber experience, and I believe Compaq and Netscape have shown that if one only wants to surf the net that one does not need an operating system - and one certainly does not need Windows - at all.

But it would be quite unrealistic to assume that the market analysts and spin doctors in Redmond have suddenly, after decades of incredibly clumsy successes, suddenly got it all wrong. A gray shadow of unreality creeps closer, hovering, threatening, foreboding, and I can literally feel it. Here we have an operating system destined to be one of the greatest and most bugged monsters of all time offering us literally nothing most of us will ever need and forcing us, moreover, to upgrade our hardware at a great expense - and all of this is _for naught_, all of this gives 95% + of the world's computer users absolutely _nothing_ - and yet we all know how things are going to go in the long run anyway, don't we?

The boggle continues. Ballmer insisted Windows 95 would run on a 386 with 4MB RAM. I knew he had to be crossing his fingers behind his

back and so I went out and bought a machine with a Pentium and a walloping 16MB RAM and it turned out I was right. Yet the quantum leap from a 386 and 4MB to a Pentium and 16MB is nothing compared to the leap expected now. I have for several years run courses in NT programming using first the NT 4 Shell Technology Update and then NT 4 itself, with MSVC running on top, with only 32MB RAM installed on low-end Pentium machines, and we have never had a hitch. We have of late attempted to demonstrate Win2K on classroom machines with far faster processors and many times the RAM and had to abandon our efforts. Windows 2000 simply peaks the CPU meter even in idle and then calmly stands still.

I keep thinking about that comment from Microsoft that another RISKS reader recounted to me: "that's not the way we do things at Microsoft - when it gets too slow we just throw more hardware at it." And for those of you that followed the ripples from these forums in the Daily Telegraph's Connect supplement, yes my company today does have that "Windows Explorer" replacement mentioned there, and it does not consume a quarter of a megabyte on disk as its Redmond counterpart, but only 26KB. 26,624 bytes. As one user wrote to us: "I can finally throw that Microsoft Windows Explorer in the trash bin where it belongs."

It is important to realize that our conditions were not better than Redmond's - quite on the contrary. We did not have access to, or ever consider availing ourselves of a staff several times the size of

Redmond's. We did not work long hours in our offices and sleep on our futons as one is expected to do in Redmond. We just wrote the program. Like anything else we write. And over a time span considerably more realistic than Redmond used for Windows Explorer.

Bloat is not unavoidable. Bloat is not a necessary evil.

Bloat is always, has always been, and will always be a totally indefensible blot on computer science.

I fail to see how anyone - even a band of zonked-out Microserfs - can take what was almost an operating system - NT - almost totally based on, if not identical with DEC's VMS, and systematically turn it into the biggest, most bloated bug farm in the history of computer science - and, for every turn in the road, for every day and week that went by, not improve the code and make the system run faster, but literally ruin the code and make the system run slower, or run not at all. I truly think that the ordinary laws of logic, of human intelligence, somehow fail to apply in the Pacific Northwest, and am starting to facetiously wonder if David Lynch wasn't onto something after all. Is Laura really Melinda French? Doesn't WHG3 have the faintest resemblance to her father, and SB a bit too much in common with Kyle's night porter?

For those fanatics who said all along we should leave the big cities, that people would drop like flies in droves from the hypothermia - I am beginning to wonder. For the first time I am getting scared of the

Millennium - and not for the COBOL bug, but for the Redmond Millennium Bug. The wife is now negotiating with the realtors at Prayer Lake to see if they will part with some of their precious real estate and thereby help save a few more lives.

PS. Anyone who wants a further peek at this "Explorer killer" of ours to see for themselves that it really can be done is welcome to drop a line at the address below. We'll send along a complimentary copy.

Rick Downes, Radsoft Laboratories <http://www.radsoft.net>

✶ You can't get where you want to go today

<jfieber@indiana.edu>

Tue, 12 Oct 1999 23:13:12 -0500 (EST)

I've had a number of experiences making me wary of route planners, though not as dramatic as those reported in 20.62 (which I have not personally verified). Most curious are the can't get there from here journeys. The latest impossible trip I booked, ultimately with the assistance of a real travel agent, was from Indianapolis USA to Glasgow Scotland on Northwest/KLM.

According to Expedia, you can't do that. According to Northwest's online booking, you can't do that. Well, of course, both appear to use the same Microsoft software. I'll grant that going to Glasgow via Amsterdam isn't the shortest way, but it is certainly possible and the only way

you are
going to get there on Northwest/KLM. I know you can get there
from here
because I've gone there from here more than once.

In the same way that Internet search engines leave me wanting to
know the
scope of their database, harvesting policies, and details of
their indexing
and retrieval machinery, travel planning services leave me
wanting to know
more of their route planning machinery. Why though? I
certainly don't
worry about the algorithms my local human travel employs.

It isn't about the imperfectness of the search. A human agent
won't always
find the optimal flight either...the first time around at
least. You see,
the human doesn't need a perfect search algorithm because the
human agent
has that amazing exception handling code known as called common
sense.

If the electronic travel agent has no common sense to spot
suspicious
results from an imperfect algorithm. When faced with a possible
failure, it
should should solicit help from the most convenient repository
of common
sense, the user. In this case, letting me tell it "Yo!
Expedia! Here is a
hint: Amsterdam is Northwest/KLM's main European hub. Maybe try
a route
through there?" would have done wonders.

But not in the World According to Microsoft where users are
idiots and
Wizards claim a monopoly on common sense. I want smart
software, but if I
can't have that, I want dumb software that knows it is dumb and
comes to me
for help, not dumb software that thinks it is smart and tells me

lies it
believes to be true.

🔥 Odd synchronicity in items in [RISKS-20.62](#)

Chris Smith <smith@interlog.com>
Thu, 14 Oct 1999 16:23:57 -0400 (EDT)

I noticed in [RISKS-20.62](#), item 17...

"Where do you want to be *mis*directed today?"

...
> From: Laurel, Maryland
> To: Baltimore-Washington International Airport, Maryland
> Driving Distance: 5865.1 miles
> Time: 9 day(s) 3 hour(s) 22 minute(s)
>
> Driving Directions
...
> 36:35 Turn left onto Local road(s) (4543.1 mi)
> 219:22 Arrive Baltimore-Washington International Airport,
Maryland

And then I noticed in [RISKS-20.62](#), item 18 (yes, the next item
[NO
COINCIDENCE THERE! PGN])...

"Maybe Microsoft owns stock in Canada?"

...
> Summary
> From: Hastings, Minnesota
> To: Saint Charles [St. Charles], Minnesota
> Driving Distance: 6758.6 miles
> Time: 9 day(s) 17 hour(s) 30 minute(s)
>
> Driving Directions
...
> 50:43 Turn left onto Local road(s) (SE 4543.1
miles)

> 233:30 Arrive Saint Charles [St. Charles],
Minnesota

Can someone tell me -- is it really 4543.1 miles from the actual location indicated to *BOTH* St.Charles, Minnesota *AND* to Baltimore-Washington Airport?

Or, similarly - if someone has the detailed directions for the first (abridged) example - do you actually end up at the same location just before the last leg?

(For both of these, we would need the unabridged directions from the first example to see if the previous location was "At Bay Bulls, turn right onto S-10".)

And might this location be the easternmost reachable point in North America by car? If so, this appears to be an implementation of that well-known solution to driving in the wrong direction; just drive around the world. Of course, once you run out of roads, it's clear that (1) you really can't just keep going, and (2) after all that driving, you must be at least close. Just take the local roads for that last little bit.

Chris Smith <smith@interlog.com>

⚡ Re: Cyber-Speak ([RISKS-20.61](#))

Martin Minow <minow@pobox.com>
Fri, 01 Oct 1999 19:53:09 -0700

Ira J. Rimson notes that printer software delivered on CD-ROM includes a utility to copy the printer drivers so they can be installed on systems that lack a CD-ROM and asks,

> Am I missing something obvious here?

The manufacturer is probably assuming that the customer has at least one computer with a CD-ROM, but that the printer may be used by other computers -- presumably on a network -- that lack a working CD-ROM drive.

The CD-ROM probably includes drivers for a variety of operating systems, as well as PDF copies of the manual, sample images, etc. etc.

CD-ROM mastering costs are quite low (on the order of \$0.50 each for 10,000 copies and one-week turnaround). I suspect that adding a floppy distribution would add about \$2 or more to the manufacturing cost without adding anything substantial to the overall usability of the product. So, from my point of view, it seems like a nice gesture on HP's part, rather than a chicken/egg problem.

Martin Minow <minow@pobox.com>

[Many other similar comments. PGN]

⚡ Bell Atlantic forgets: exchanges are not unique between area codes

"Jonathan I. Kamens" <jik@kamens.brookline.ma.us>
Fri, 8 Oct 1999 14:50:58 -0400

I received a mailing from Bell Atlantic yesterday which was entitled,
"Important Notice for our Brattleboro (254, 257, 258) Exchange Customers."
It starts out:

Because of growth in the number of telephone lines in your local calling area, your exchange will be changed from rate group 6 to 7, and rates will be affected as described below.

Under the Vermont tariff (P.S.B. - Vt. - No. 20 Part A, Section 5.1.3) exchanges are classified by rate groups according to the number of telephone lines in the local calling area....

The problem is that I don't live in Brattleboro. I don't even live in Vermont.

It would appear that a Bell Atlantic DB Admin searched for all Bell Atlantic telephone numbers starting with 254, 257 and 258, regardless of area code. How much do you think they wasted in postage and printing costs to send out all those bogus notices? How many hours are going to be wasted by customer service representatives answering questions about them? And why didn't somebody realize that the number of notices being sent out was more than the number of customers which could fit in three exchanges?

I spoke to a very friendly Bell Atlantic customer service representative who said that she didn't know exactly how widespread the problem was, but she confirmed that at the very least it went out incorrectly to all Massachusetts "254" customers. On the bright side, she confirmed that it also went out to all the people who were supposed to receive

it. She also said she thought the mailing created "job security" for people like her.

The unamusing thing about all this is that our telephone rates go up to pay for stupid blunders like this one.

Jonathan Kamens

⚡ Yet another case of credit-card 'security'

E. Lange <el@qua.crl.melco.co.jp>

Fri, 1 Oct 99 20:46:03 JST

Recently I received a new credit card by mail, as an old card was soon to expire. The envelope was strangely mangled: both the outline of the credit card and the embossed numerals and letters on the card were clearly impressed in the envelope and the three layers of paper between envelope and credit card.

My best guess: someone must have taken an impression of the credit card through the envelope! (The pressure must have been high, as even the black paint on the embossed numerals and letters had partially been transferred to the enclosed letter.)

Needless to say, I called the credit card company and cancelled the credit card before it became active. I offered to send in the mangled envelope, but the representative said she wouldn't know what to do with it, and that she had not heard of any similar case.

The risks: 1) This way of transportation is unsafe: credit card information can be captured in transit with primitive means; at least some cardboard would be needed to make sure that cards can not be imprinted through the envelope. 2) There seems to be no information gathering and warning system in place to stop new scams (possibly with high criminal energy) in its tracks.

And the non-risk: unencrypted credit card transmissions might be *comparatively* safe, after all...

✶ CFP: FTCS-30 & DCCA-8 Int'l Conf on Dependable Systems and Networks

Philip Koopman <koopman@cmu.edu>
Fri, 15 Oct 1999 17:41:00 -0400

CALL FOR CONTRIBUTIONS

The International Conference on Dependable Systems and Networks

(FTCS-30 and DCCA-8)

New York City, NY

June 25-28, 2000

<http://www.dependability.org>

Conference Submission Deadline: November 5, 1999
Workshop Submission Deadlines: see <http://www.dependability.org>

The International Conference on Dependable Systems and Networks represents a new beginning in the field of dependable computing, as well as the

continuation of long-established traditions. Formed from the combination of two established conferences - the International Symposium on Fault-Tolerant Computing (FTCS) sponsored by the IEEE Computer Society and the Working Conference on Dependable Computing for Critical Applications (DCCA) sponsored by IFIP WG 10.4 - this inclusive conference is designed to capture the wide range of activities in this increasingly important technical area. The conference scope spans system, software, hardware, and network issues. Major topics include, but are not limited to, Architectures for Dependable Computer Systems; Transaction Processing; Fault Tolerance in Distributed, Mobile, and Real- Time Systems; Safety-Critical Systems; Dependability of High- Speed Networks and Protocols; Quality of Service; Fault Tolerance in Multimedia Systems; Software Reliability, Fault Tolerance, Testing, Validation, and Verification; Dependability Modeling and Prediction; and Dependability in VLSI.

For information and submission deadlines about the events comprising the International Conference on Dependable Systems and Networks, check <http://www.dependability.org> .

Conference General Chair:

T. Basil Smith (USA) tbsmith@us.ibm.com

Conference Program Chairs:

Doug Blough (USA) doug.blough@ece.gatech.edu
Karama Kanoun (France) kanoun@laas.fr

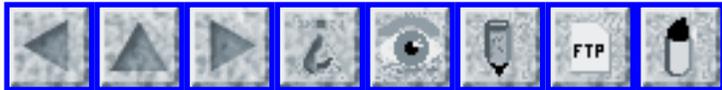
Workshop on Dependability despite Malicious Faults Program Chair:

Yves Deswarte (France) deswarte@laas.fr

Workshop on Dependability of e-business Systems Program Chair:
Nick Bowen (USA) bowenn@us.ibm.com

Workshop on Dependability of IP Applications, Platforms and
Networks

Program Chair:
Yennun Huang (USA) yen@research.att.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 20: Issue 64

Thursday 4 November 1999

Contents

- [Yet another cracked stoopid crypto scheme...](#)
[Frank Stevenson via Lenny Foner](#)
- [A Risk of disk caching](#)
[Erling Kristiansen](#)
- [Single-Sourcing at the FAA](#)
[Eriks A Ziemelis](#)
- [Re: Aircraft computer redundancy, airline safety](#)
[Paul Wallich](#)
- [Re: Y2K creates "horseless carriages"](#)
[Ted Doty](#)
- [Cornell University Revisits Spring 1900](#)
[James Byers](#)
- [Bush campaign site hacked](#)
[Avi Rubin](#)
- [IP blocking](#)
[Lindsay Marshall](#)
- [INS Irony Explained](#)
[Paul Robinson](#)
- [Fibers Cut in Massachusetts](#)
[Rich](#)

- [Typing fast, and a fast computer are not necessarily good!](#)
[Vicky Larmour](#)
 - [Printers are too smart to handle "dumb" jobs](#)
[Leonard Erickson](#)
 - [Complexity in operating systems and programming languages](#)
[Diomidis Spinellis](#)
 - [Re: DC Metro Relays](#)
[David Lesher](#)
 - [BlackICE Defender Security woes](#)
[tlb](#)
 - [10-day deactivation warning from Network Solutions takes 13 days](#)
[Stuart Woodward](#)
 - [40 vs. 128 bit browsers](#)
[Jeremy Epstein](#)
 - [New Australian RISKS Archive](#)
[WestyX](#)
 - [Call for papers, Malicious Information Technology](#)
[Jeffrey Voas](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Yet another cracked stooopid crypto scheme...

Lenny Foner <foner@media.mit.edu>

Wed, 27 Oct 1999 12:00:52 -0400 (EDT)

...and yet another example of why security through obscurity, not to mention non-peer-reviewed design of cryptosystems, is just dumb. Not, I imagine, that anyone but the vendors is going to complain.

This means that DVD encryption can be cracked is something like a tenth of a second. And the next message in the thread points out that the known plaintext part is easy, too.

[Note: if you follow the URL, it appears that the message got automatically mangled by the software that threads messages into web pages; the .Z has many mailto:'s that shouldn't be there...]

- - - Begin forwarded message - - -

Date: Wed, 27 Oct 1999 14:54:17 +0200 (CEST)
>From: Frank Andrew Stevenson <frank@funcom.com>
To: cryptography@c2.net
Subject: CSS broken

Monday sourcecode for the CSS algorithm was released through an anonymous remailer. CSS is the encryption algorithm used on DVD movies, and it was suspected that it was weak beyond just having a 40 bit key. Yesterday I found it to be vulnerable to a trivial 2^{16} attack with as little as 6 bytes of known plaintext.

I posted the details on:
<http://livid.on.openprojects.net/pipermail/livid-dev/1999-October/000589.html>

frank

A Risk of disk caching

Erling Kristiansen <ekristia@xs4all.nl>
Fri, 22 Oct 1999 20:01:52 +0200

I do most of my typing in Frame Maker on a UNIX system. When I send documents, I print to a pdf file and attach it to an Email.

My company uses Lotus Notes as our standard mail platform. For

most
users, including myself, Notes runs on a Win95 platform. My PC
mounts
the disk of the UNIX system as a network drive, so I can include
the pdf
attachment directly from the UNIX disk into Notes.

Today, I did just that.

The recipient called me with a few modifications to the document
I had
just sent him.

I did the modifications, and repeated the process of generating
pdf and
attaching to an email. Note that, in this process, the new pdf
file
replaced the old one. The old file therefore no longer existed
explicitly anywhere.

The recipient called me and said: You sent me the old version of
the
document. Can I please have the updated one.

I investigated a bit, and discovered that, consistently, once a
file
with a given name has been included as a Lotus Notes attachment,
this
version of the file will be attached to subsequent mails that
call for
this attachment, even if the contents of the original file has
changed!

Though I have not attempted to understand the deeper logic of
this, it
looks like a disk caching that is unaware that somebody else may
have
changed a file on a networked drive, so it gives you the cached
version
whenever this file is called for.

In this case, no harm was done, but I can imagine quite a few
"nice"

scenarios resulting from obsolete files being distributed instead of current versions.

✈ Single-Sourcing at the FAA

Eriks A Ziemelis <eazy@ecae.stortek.com>

Thu, 21 Oct 1999 08:58:17 -0600

From "The Chicago Tribune", 10/21/1999:

<http://chicagotribune.com/news/metro/chicago/article/0,2669,ART-36492,FF.html>

Thomas A. Varlotta stands accused of destroying the lone copy of source code for a system to transfer flight control data between the control tower at O'Hare airport and a control center in Elgin, IL. Luckily, in a raid on Varlotta's home, authorities recovered an encrypted copy of the source code and managed to decrypt it in six months. Otherwise, 3-5 more years to rewrite the software.

Quote the FAA: "It's an efficiency issue, not a safety issue."

Paraphrasing the Department of Transportation investigator: Why did only one person have the source code? "I'm just a layman," Harper said. But "that doesn't sound like a good business practice," he said.

Comment #1: Not a safety issue? The old method of transferring data, according to the article, was via telephone. Someone mishears and/or transcribes the data incorrectly, anything in place to catch problems when a

controller call out the wrong plane, a dangerous course
correction/altitude
change? Maybe not a safety issue, but, not comforting.

Comment #2: Noone heard of backups at the FAA? Varlotta was not
working
alone on the project: noone else had a copy? FAA is not backing
up their
software? We backup our software here every night and I still
make a backup
of my own every other day, just to be analy-safe.

✈ Re: Aircraft computer redundancy, airline safety (Olson, [RISKS-20.63](#))

Paul Wallich <pw@panix.com>
Sun, 17 Oct 1999 10:21:04 -0400

There are a lot of redundant items in your typical aircraft
cockpit so that
the plane doesn't fall out of the sky if one of them fails. If
memory
serves, the A320 has three flight computers, any one of which
can handle the
aircraft. Flying with two out of three would not then be a
problem, even if
you would prefer all of them functioning for maximum
reliability. (And one
would expect that the confused box would be swapped out or
otherwise fixed
overnight, without as much inconvenience to passengers.)

What would be a problem would be flying with one of your flight
computers in
operation but malfunctioning so that there would be arguments
among them
about what the plane was doing.

Paul Wallich

pw@panix.com

⚡ Re: Y2K creates "horseless carriages" (Griffith, [RISKS-20.63](#))

"Doty, Ted (ISSAtlanta)" <TDoty@iss.net>

Thu, 21 Oct 1999 18:48:36 -0400

>AP reports that a Y2K glitch has caused 2000 new vehicle registrations in
>the state of Maine to bear the classification "horseless carriage".
>Apparently, the DMV software misread the 2000 model year as 1900, and it is
>hardwired to classify any vehicle with a model year before 1916 as a
>horseless carriage.

This smells like an urban legend. Can you imagine a programmer at the DMV titling a category as "horseless carriage", or even a faceless bureaucrat specifying that name? It's unlikely that the DMV was computerized earlier than the 1960s, and that term just doesn't sound likely.

><http://www.mercurynews.com/breaking/docs/024281.htm>"

---This link is dead, adding to the suspicion. I think someone was pulling their legs (successfully), and they got caught.

- Ted

Ted Doty, Internet Security Systems | Phone: +1 678 443-6000
6600 Peachtree Dunwoody Road, 300 Embassy Row | Fax: +1 678 443-6479
Atlanta, GA 30328 USA | Web: <http://www.iss.net>

✶ Cornell University Revisits Spring 1900

James Byers <jwb19@cornell.edu>

Tue, 19 Oct 1999 14:47:05 +0000

On 16 Oct 1999, Cornell University seniors registering for classes via the online CoursEnroll system were greeted by the following splash screen text:
"Use this service to enter your pre-enrollment requests for the Spring 1900 semester." Following this screen, the main application window proclaimed in a large font: "CoursEnroll for Spring 1900." The glitch was quickly corrected.

The relevant Cornell Y2K status page (<http://www.cit.cornell.edu/y2k/services.html>) states the service (Just the Facts) will be compliant sometime in October 1999. Enumerating the usual set of Y2K jitters is an exercise left to RISKS readers.

On the bright side, perhaps Cornell will finally offer those long-awaited classes in horseless carriage design come spring...

James Byers (jwb19@cornell.edu)

✶ Bush campaign site hacked

Avi Rubin <rubin@research.att.com>

Wed, 20 Oct 1999 11:56:51 GMT

>From the AP news wire:

The day after presidential candidate George W. Bush redesigned his campaign's Web site, hackers vandalized it by replacing his photo with a hammer and sickle and calling for "a new October revolution."

Avi Rubin

⚡ IP blocking

<Lindsay.Marshall@newcastle.ac.uk>

Mon, 18 Oct 1999 13:08:04 +0100 (BST)

This was brought to the attention of readers cam-list recently:

<<http://www.zdnet.com/zdnn/stories/news/0,4586,2352917,00.html>>

"For a month or so earlier this year, DoubleClick Inc., an Internet advertising firm based in New York, furtively put up three different editions of its home page. Most visitors saw one version, highlighting the firm's accomplishments. Employees of a rival firm could see only another version, with a special press release touting DoubleClick's capture of one of the rival's customers. Clients being wooed saw only a third version."

⚡ INS Irony Explained

<Rfc1394a@aol.com>

Mon, 18 Oct 1999 06:31:21 EDT

Someone wrote to ask me about the article I posted to Risks. Since the irony was not evident to someone it might not be evident to others so I thought I'd explain for the benefit of those who might not get it

I wrote,

>> The following item was reported in the UK's Silicon.Com weekly round-up:

>>

>> The US government admitted this week that it had accidentally issued

>> more visas for foreign high-tech workers than it had intended - 20,000

>> to be precise. Why? Because of a computer glitch. Irony once again

>> rears its ugly head and slaps the authorities around the face with a wet fish.

To which a reader replied:

> Apart from the irony, I wonder why this is a problem? World-wide there

> are not enough high-tech workers, so getting an extra 20,000 sounds

> to me like a bonus not a problem.

The irony being that too many trained technical people, such as computer programmers, were admitted than were allowed by law, yet it implies that INS apparently does not have enough trained computer programmers to keep this sort of mistake from happening!

Paul Robinson <rfcl394a@aol.com>

Fibers Cut in Massachusetts

<rich@wisdom.wsc.ma.edu>

Mon, 18 Oct 1999 10:30:36 -0400

> From our ISP:

> At about 2:30am Saturday morning (10/16) a catastrophic fiber
> cut occurred
> on the Mass Turnpike. Literally, the classic backhoe
> scenario. AT&T (288
> strands), MCI Worldcomm (12 strands) and the MTA (Mass
> Turnpike Authority,
> don't know how many strands but MITI's are among them) had
> their fiber
> severed. This is an outage affecting people all up and down
> the east
> coast. Don't be surprised if your bank machine won't dispense
> you cash
> today.

✶ Typing fast, and a fast computer are not necessarily good!

Vicky Larmour <vicky.larmour@camcon.co.uk>

Wed, 20 Oct 1999 14:23:05 +0100

I often wish I could type faster, and that I had a faster
computer, but
yesterday I wished my typing was slower and I had a slower
computer!

I was inputting some text (ironically, software test details!)
into an
Excel 97 spreadsheet by typing the contents of one cell,
pressing return,
typing the contents of the next cell down, etc.

All was going well until suddenly, seemingly without warning, my
Excel
window simply disappeared and I was left wondering what on earth
was going
on. I re-started Excel and discovered I had lost an hour's
rather tedious
work, so I set about trying to work out why. After a little
probing, it

dawned on me. At the time Excel disappeared, I had been entering the text

```
// cannot be tested in test harness  
in a cell.
```

This is what happened as I typed that text:

- Evidently, Excel 97 treats a forward slash as an ALT press (highlighting the File menu button), if a cell is selected but not being edited.
- the second forward slash was ignored
- the space key caused the application window menu to drop down.
- the "c" selected the "close" option from that menu, which brought up a dialog box saying "Do you want to save? Yes / No / Cancel".
- the "a" was ignored
- the "n" activated the "No" option on the dialog box.
- poof! Excel closed without saving.

All this happened in the blink of an eye, as I typed, so I didn't even get to see the dialog box that might have stopped me in my tracks. It was only by careful reconstruction of exactly what I had been doing that I worked out what had happened.

The RISKS? Undocumented and inconsistent keyboard shortcuts - why should forward slash be treated as an ALT press, but not if I am already editing text in a cell? Why isn't this listed in the keyboard shortcuts in the Excel help?

[Extra RISK: My work hadn't been auto-saved because in Excel 97, you have to install the AutoSave Add-in if you want auto-save, which isn't something I had explicitly thought to do (but now have!). If Auto-save had been an item on the tools menu from the start, I might well have noticed it and

switched it on!]

Vicky

✶ Printers are too smart to handle "dumb" jobs

Leonard Erickson <shadow@krypton.rain.com>

Sat, 16 Oct 1999 23:39:19 PST

There's been an interesting discussion going on on Fidonet's TECHNICAL echo recently. It started when an echo participant asked if anyone knew of **new** printer models that could merely be hooked up to a standard printer port and used to dump text data to.

Why was he asking? Because he'd just had the customer service departments of **every** printer company he called, said that their current model printers **will not** print except under Windows, with appropriate drivers loaded!

Since he works for the military, and was trying to come up with a printer his section could recommend for dumping logging data from some embedded (and very much **non** Windows) equipment, this was somewhat less than useful.

Further checking has come up with **one** printer line, and that one is expensive industrial grade equipment intended for very heavy use.

However, tests by some readers have shown that **some** "current model" printers **will** print plain text just fine. But others that are ostensibly the "same model" won't.

The risk? Windows has become so common that an important piece of hardware is in danger of becoming unusable **without** it. At least unless you can guarantee a **huge** market or afford custom orders.

Or, more likely, Windows has become so prominent that it's impossible to get a **non**-Windows answer from customer support.

Either way, this is going to become a real problem as more older printers go out of service.

I **was** thinking about throwing out some old Epson printers. Now I think I'll hold onto them.

Leonard Erickson (aka Shadow) shadow@krypton.rain.com

✶ Complexity in operating systems and programming languages

Diomidis Spinellis <dds@sena.gr>
Mon, 18 Oct 1999 12:02:11 +0300

A number of contributors to previous digests have stressed the risks associated with increasingly bloated software applications. Unfortunately the same issues permeate a number of facets of the software industry. Consider operating systems and programming languages which are becoming increasingly complicated and their implementations less trustworthy. The following table [1] contains the number of documented system calls for some popular Un*x system versions:

Operating System	Year	Number of system calls
First Edition Unix	1971	33
Seventh Edition Unix	1979	47
SunOS 4.1	1989	171
4.3 BSD Net 2	1991	136
HP-UX 9.05	1992	219
SunOS 5.4	1994	163
Linux 1.2	1996	211
SunOS 5.6	1997	190
Linux 2.0	1998	229

The Windows platform with 3433 API calls (up to NT4 SP3) belongs to a different league; the associated problems are documented elsewhere [2].

A system call defines an interface to the operating system; more system calls increase the complexity of the operating system needed to support them, provide additional opportunities for unwanted interactions between them, and increase the chances of overlooked security loopholes.

This increasing complexity has important implications for the reliability of software developed for a specific platform. Complicated interfaces are difficult to learn and use effectively. As a result of their size and complexity, modern operating systems exhibit an increasing number of bugs; demonstrated by the numerous "fixes" distributed by their vendors.

Developers of robust applications have to take this into account coding around them, or insist on the installation of all relevant fixes. Some fixes may introduce new errors or render other system components inoperative. The bottom-line of this situation is, that the application developer is practically rarely singly responsible for the

reliability of an application.

Similarly to operating systems, programming languages also have a tendency to grow in size and complexity as they mature. Taking as a rough measure the page number of the language's canonical description the following table provides an illustration of the evolution of the C and C++ programming languages:

Book Title	Year	Pages
The C Programming Language (Kernighan and Ritchie)	1978	228
The C Programming Language; second edition	1988	272
The C++ Programming Language (Stroustrup)	1986	328
The C++ Programming Language; second edition	1991	669
The C++ Programming Language; third edition	1997	910

This trend has important implications for the developers of high-reliability systems. Large languages are difficult to learn and use [3]. It is nowadays not uncommon for programming teams to lack people who understand the whole language at a level sufficient to advise other members on issues regarding the interrelationship between language elements. Subtle bugs arising from the misunderstanding of language features can thus survive code walkthroughs. In addition, language complexity and advanced optimisation techniques combined with processor complexity results in an increased number of bugs in modern compilers. This is clearly an additional risk factor for high-reliability designs.

[1] Diomidis Spinellis. Software reliability: Modern challenges. In G. I. Schueller and P. Kafka, editors, Proceedings ESREL '99 - The Tenth

European Conference on Safety and Reliability, pages 589-592, Munich-Garching, Germany, September 1999. ESRA, VDI, TUM, A. A. Balkema.

<http://kerkis.math.aegean.gr/~dspin/pubs/conf/1999-ESREL-SoftRel/html/chal.html>

[2] Diomidis Spinellis. A critique of the Windows application programming interface. *Computer Standards & Interfaces*, 20:1-8, November 1998.

<http://kerkis.math.aegean.gr/~dspin/pubs/jrnl/1997-C SI-WinApi/html/win.html>

[3] C. A. R. Hoare. Hints on programming language design. In Ellis Horowitz, editor, *Programming Languages: A Grand Tour*, pages 31-40.

Computer Science Press, 1983. Reprinted from Sigact/Sigplan Symposium on Principles of Programming Languages, October 1973.

Diomidis Spinellis, University of the Aegean

⚡ Re: DC Metro Relays ([RISKS-20.63](#))

David Leshner <wb8foz@nrk.com>

Thu, 21 Oct 1999 11:15:01 -0400 (EDT)

> The Washington DC Metro has had rampant failures among its electronic
> relays, and as a result has been running the entire system manually ...

Note these appear (from past press photos & descriptions) to be time-proven, dirt-ordinary, railroad-standard relays, such as have been used since oh, the era of Tom Thumb and/or the Golden Spike.

Everyone talking has been head-scratching; metallurgists and other specialists consulted to no avail.

We spend a lot of time in RISKS discussing new, unproven, technologies & the dangers lurking within same. But this appears to be an old old one that suddenly has fallen into the gutter for reasons unknown. I find this very disturbing.

⚡ BlackICE Defender Security woes

"tlb" <tomeuchre@yahoo.com>
17 Oct 1999 03:48:31 GMT

I just recently purchased the BlackICE defender program to protect my computer against internet hackers and other co-workers. While scanning the unprotected, unencrypted raw logs of the program, what do you think I found? The SMTP dialog between my mail program and my Mail server, complete with the account and password right out there in the open. Quite ironic that a company selling a product to ensure security and system integrity actually created a gaping hole. braz@mnw.net (a 2-day user of BlackICE Defender -- the product won't see 3 days on my machine).

⚡ 10-day deactivation warning from Network Solutions takes 13 days

Stuart Woodward <stuart@gol.com>
Sat, 30 Oct 1999 13:55:29 +0900

Due to an oversight on my behalf, payment to Network Solutions for the renewal fee for one of my domains was overlooked and in time I received a reminder that it needed to be paid. The reminder comes via an ordinary postal letter. So as soon as I got the reminder, I logged on and paid the fee at the Network Solutions website.

Since the postal letter took some time to arrive, a Deactivation Notice from Network Solutions had already been dispatched. When it arrived today it gave me a fright because the letter, giving me a final 10 days to pay, was dated 17th October 1999 and it only arrived here in Japan via Amsterdam (!) on the 30th of October.

To me this poses two questions: Why doesn't Network Solutions send an e-mail reminder to the Billing Contact when they send out the postal mail and why do they use such a slow postal delivery service for such time sensitive information?



✶ 40 vs. 128 bit browsers

Epstein Family <jepstein@mail.mnsinc.com>
Mon, 18 Oct 1999 20:35:53 -0400

Wells Fargo administers the 401(k) for a previous employer, where I still have an account. Today I received a letter which reads in part:

"We have, from our initial introduction of Internet access to retirement account information nearly two years ago, recognized the value

of requiring users to utilize browsers that support the strong, 128-bit encryption available in the United States and Canada. Following recent testing of an upgrade to our Internet server, we discovered that the site had been put into general use allowing access with standard 40-bit encryption. We fixed the problem as soon as it was discovered, and now, access is again only available using 128-bit encryption. ... We have carefully checked our Internet server and computer files and determined that at no time was the site accessed without proper authorization while we were using the standard encryption program. ... We have adjusted our server monitoring to test for lower encryption on an hourly basis to ensure the server is maintained at the highest encryption level for your protection."

I found this to be both reassuring (that they admitted the error) and frightening (that they state so confidently that the site was never accessed improperly, which seems a trifle strong assertion). I was also pleased to see that they're now testing for recurrences of this configuration error on a regular basis.

The letter then goes on to explain that there's no indication to IE users to indicate whether they're using 40-bit or 128-bit encryption, but Netscape 4.0 & later users can click on an icon to see the type of crypto.

While there's no explanation of how this configuration error occurred, it shows the risk of systems that **appear** secure (i.e., using 128 bit

encryption), when they're really not (i.e., using 40 bit encryption). Even a reasonable effort to look at the output of the system would appear encrypted in either case; it's only if someone took a closer look at the traffic that the discrepancy would occur. Compounding this is the fact that it's not obvious (or even available) to users whether they're using a strong or weak system, and an error will go undetected a long time.

Moral of the story: if it's easy to misconfigure a system so it's insecure, that's exactly what will happen.

--Jeremy Epstein

New Australian RISKS Archive

Ochran Industries <n2585464@sparrow.qut.edu.au>
Mon, 18 Oct 1999 20:08:27 +1000 (EST)

There is now an Australian mirror of risks at

<http://mirror.aarnet.edu.au/risks/>

This is a html page of the ftp files, and contains all risks issues up to [risks-20.61](#) (02-Oct-1999).

westyX - n2585464@sparrow.qut.edu.au

Call for papers, Malicious Information Technology

"Jeffrey M. Voas" <jmvoas@rstcorp.com>

Fri, 22 Oct 1999 15:51:57 -0400

Co-Authored:

Software Assessment: Reliability, Safety, and Testability
(Wiley, 1995)

<http://www.rstcorp.com/books/sa>

Software Fault Injection: Inoculating Programs Against Errors
(Wiley, 1998) <http://www.rstcorp.com/books/sfi>

Videos:

Developing Software for Safety Critical Systems
(IEEE, 1998) http://www.rstcorp.com/videos/safety_critical.html

Software Testing: Building Infrastructure, Due Dilligence, and OO
Software
(IEEE, 1999) http://www.rstcorp.com/videos/software_testing.html

IEEE Software

Call for Articles & Reviewers

Malicious Information Technology: The Software vs. The People
Publication: Sept./Oct. 2000

Software was intended to improve the quality of human life by doing tasks more quickly, reliably, and efficiently. But today, a "software vs. people" showdown appears eminent. Software is increasingly becoming a threat to people, organizations, and nations. For example, the spread of the Melissa virus illustrates the ease with which systems can be penetrated and the ubiquity of the consequences; the Melissa virus caused many companies to shut down their EMail systems for days or even weeks. The origin of these threats stems from a variety of problems. One problem is negligent development practices that lead to defective software. Security vulnerabilities that occur

as a result of negligent development practices (e.g., commercial Web browsers allowing unauthorized individuals to access confidential data) are likely to be discovered by rogue individuals with malicious intentions. Other security vulnerabilities are deliberately programmed into software (e.g., logic bombs, Trojan Horses, and Easter eggs). Regardless of the reason why information systems are vulnerable, the end result can be disastrous and widespread.

Because of the increased danger that malicious software now poses, we seek original articles on the following specific issues:

- + Intrusion detection
- + Information survivability
- + Federal critical infrastructure protection plans
- + Federal laws prohibiting encryption exports vs. US corporations
- + State-of-the-practice in security testing
- + The Internet's "hacker underground"
- + Corporate information insurance
- + Penalties for those convicted of creating viruses
- + Case studies in information security and survivability

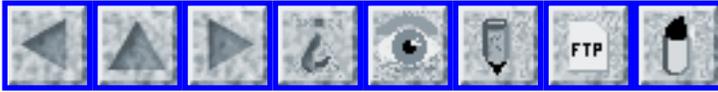
Submissions due: 1 April 2000

Guest Editors:

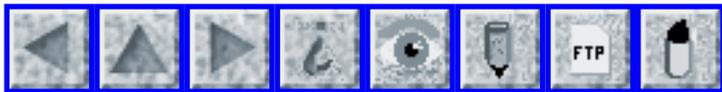
Nancy Mead	Jeffrey Voas
Carnie Mellon University	Reliable Software Technologies
nrm@sei.cmu.edu	jmvoas@rstcorp.com

Authors: Submit one electronic copy in RTF interchange or MS-Word format and one PostScript or PDF version to the magazine assistant at software@computer.org. Articles must not exceed 5,400 words including tables and figures, which count for 200 words each. For detailed author guidelines, see www.computer.org/software/edguide.htm. Reviewers: Please e-mail your contact information and areas of interest to a guest editor.

Jeffrey M. Voas, Co-Founder, Reliable Software Technologies,
Suite 400,
21351 Ridgetop Circle, Dulles, VA 20166 USA, jmvoas@rstcorp.com,
Phone: 703.404.9293, Fax: 703.404.9295



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 65

Sunday 21 November 1999

Contents

- [Nasdaq software failure](#)
[Keith A Rhodes](#)
- [Netscape's cookie-preserving behavior](#)
[Crispin Cowan](#)
- [Announcing - PFIR: "People For Internet Responsibility"](#)
[Lauren Weinstein](#)
- [Businesses could owe millions for popular Year 2000 bug fix](#)
[Keith A Rhodes](#)
- [Japan rail ticket system crash due to 11/11/11 11:11](#)
[Dave Fossett](#)
[Hiroshi Naito](#)
- [Computer prompts increase errors?](#)
[Ursula Martin](#)
- [Re: Y2K creates "horseless carriages"](#)
[Adam Elman](#)
- [Possible risks in not examining end-user license agreements?](#)
[Anthony Garcia](#)
- [Microsoft Y2K liability](#)
[Lloyd Wood](#)
- [Risks of Office 2000](#)

[Lloyd Wood](#)

- [Re: Sarah Flannery](#)
[Jean-Jacques Quisquater](#)
 - [Slashes in spreadsheets](#)
[Kent Quirk](#)
 - [DVD crypto was intended to be weak](#)
[M Seecof](#)
 - [Amazon password change requests poorly authenticated](#)
[Andrew R. Thomas-Cramer](#)
 - [Who protects me from the protectors?](#)
[David Mediavilla](#)
 - [Bill Royds" <broyds@home.com>](#)
 - [Risks of advertisements in software](#)
 - [Workshop on Freedom and Privacy By Design](#)
[Lorrie Cranor](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Nasdaq software failure**

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

Wed, 17 Nov 1999 08:30:22 -0500

Traders were unable to buy or sell stocks for 17 crucial minutes on 16 Nov

1999 after Nasdaq officials attempted a software upgrade on the fly in the

last half hour of trading. Something went wrong and investors were the ones

who paid the price. [Source: Poorly timed software upgrade paralyzes Nasdaq,

by Larry Barrett ZDII, 16 Nov 1999]

⚡ **Netscape's cookie-preserving behavior**

Crispin Cowan <crispin@cse.ogi.edu>

Thu, 04 Nov 1999 18:09:33 +0000

I normally run with cookies completely disabled. Sometimes I hit sites that insist on using cookies (e.g. slashdot's login for non-anonymous posting) and so I temporarily enable cookies. I observed (with joy) that when I disable cookies again, the "cookies" file disappears from my ~/.netscape directory. Good, it appears to delete cookies when I disable them. So I started telling people about this cool feature.

However, some time later Gil Niger reported back to me that Netscape is actually preserving cookie information across bouts of disabling cookies.

Consider this experiment:

- * enable cookies
- * browse a cookie-using site
- * observe the cookies file--hmmm, it seems to contain an old cookie from
the washingtonpost.com
- * disable cookies
- * observe that the cookies file is gone, and a grep of the .netscape
directory failed to show the washingtonpost.com cookie in any file
- * re-enable cookies
- * browse another cookie-using site (not washingtonpost.com)
- * observe the cookies file again--the washingtonpost.com
cookie is back
again

Not a huge deal, but it seems misleading, at best, to *appear* to be deleting cookie information, while actually preserving it. However, I have never seen any NS documentation that suggested that NS was actually

deleting cookie info when cookies are disabled, so it's just my inference from watching the file disappear.

I can't wait for Mozilla to stabilize: I really want that "anonymous mode" feature.

My version: Netscape Communicator 4.7 for Linux/libc5/strong crypto.

Crispin

P.S. Amusing note: NS 4.7's spelling checker just flagged "Mozilla" as an unrecognized word :-)

Crispin Cowan, CTO, WireX Communications, Inc. <http://wirex.com>

Free Hardened Linux Distribution: <http://immunix.org>

🚀 Announcing - PFIR: "People For Internet Responsibility"

Lauren Weinstein <lauren@vortex.com>
Tue, 16 Nov 99 09:34 PST

ANNOUNCING
PFIR: "People For Internet Responsibility"
<http://www.pfir.org>

November 16, 1999

PFIR is a global, grassroots, ad hoc network of individuals who are concerned about the current and future operations, development, management, and regulation of the Internet in responsible manners. The goal of PFIR is

to help provide a resource for individuals around the world to gain an ability to help impact these crucial Internet issues, which will affect virtually all aspects of our cultures, societies, and lives in the 21st century. PFIR is non-partisan, has no political agenda, and does not engage in lobbying.

PFIR has been founded in November, 1999 by Lauren Weinstein of Vortex Technology in Woodland Hills, California and Peter G. Neumann of SRI International in Menlo Park, California. Both have decades of continual experience with the Internet and its ancestor ARPANET, Lauren originally at the UCLA lab which was the ARPANET's first site, and Peter at the net's second site, located at SRI.

Peter is the chairman of the ACM (Association for Computing Machinery) Committee on Computers and Public Policy, and the creator and moderator of the Internet RISKS Forum. Lauren is a member of that same committee, and he is the creator and moderator of the Internet PRIVACY Forum.

With the rapid commercialization of the Internet and its World Wide Web during the 1990's, there are increasing concerns that decisions regarding these resources are being irresponsibly skewed through the influence of powerful, vested interests (in commercial, political, and other categories) whose goals are not necessarily always aligned with the concerns of individuals and the people at large. Such incompatibilities have surfaced in areas including domain name policy, spam, security, encryption, freedom

of speech issues, privacy, content rating and filtering, and a vast array of other areas. New ones are sure to come!

While corporate, political, and other related entities most certainly have important roles to play in Internet issues, it is unwise and unacceptable for their influences to be effectively the only significant factors affecting the broad scope of Internet policies.

There are numerous examples. While e-commerce can indeed be a wonderful tool, it is shortsighted in the extreme for some interests to treat the incredible creation that is the Internet as little more than a giant mail order catalog, with ".com" associated hype on seemingly every ad, billboard and commercial. Protection of copyrights in a global Internet environment, without abusive monitoring, is a challenge indeed. The Internet can be a fantastic tool to encourage the flow of ideas, information, and education, but it can also be used to track users' behaviors and invade individuals' privacy in manners that George Orwell never imagined in his "1984" world.

PFIR is a resource for discussion, analysis, and information regarding Internet issues, aimed at providing a forum for *ordinary people* to participate in the process of Internet evolution, control, and use, around the entire world. PFIR is also a focal point for providing media and government with a resource regarding Internet issues that is not controlled by entities with existing major vested financial, political, or other

interests. This is accomplished through the PFIR Web site, the handling of telephone and e-mail queries, and through digests, discussion groups, reports, broadcast and Internet radio efforts, and other venues.

For full details about People For Internet Responsibility, including information regarding how you can participate in or keep informed about PFIR activities (including the PFIR Digest mailing list), please visit the PFIR Web site at:

<http://www.pfir.org>

Individuals, organizations, media, etc. who are interested in more information regarding PFIR or these Internet issues are invited to contact:

Phone, Fax, or E-mail:

Lauren Weinstein
TEL: +1 (818) 225-2800
FAX: +1 (818) 225-7203
lauren@pfir.org

Please send any physical mail to:

PFIR c/o Peter G. Neumann
Principal Scientist
Computer Science Lab
SRI International EL-243
333 Ravenswood Ave.
Menlo Park, CA 94025-3493 USA

Thank you very much. Be seeing you!

Lauren Weinstein
Peter G. Neumann
16 November 1999

⚡ Businesses could owe millions for popular Year 2000 bug fix

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

Fri, 12 Nov 1999 14:21:46 -0500

It turns out the windowing technique used frequently by Y2K remediators to postpone the Y2K problem (reinterpreting two-digit dates ij: from 00 to xy as 2000+ij, and from xy+1 to 99 as 1900+ij) was patented in 1998 by Bruce Dickens, at McDonnell Douglas Corp, now Boeing. He wants to collect big-time. However, that technique seems to have existed long before the patent application was submitted (for example, in the 1960s on one-digit year software). I guess we'll have to wait and see what happens. (There are apparently also 30 other much more specific patents on Y2K fixes.)
[Source: Associated Press item by Anick Jesdanun, 11 Nov 1999; PGN-ed]

[NOTE: It will be interesting if the companies then ask Mr. Dickens to fix the problem after the window expires. Keith]

[The patent office seems to be overwhelmed these days, and is issuing many patents for which prior art CLEARLY existed at the time. The entire patent process seems to be getting out of control. PGN]

⚡ Japan rail ticket system crash due to 11/11/11 11:11

Dave Fossett <dajf@REMOVE_THISpo.teleway.ne.jp>

Fri, 12 Nov 1999 14:18:04 +0900

Newsgroups: misc.transport.rail.misc

The MARS ticket reservation computer system for the nationwide JR network crashed spectacularly at 11:10 on the 11th November 1999. The reason was not initially clear, but while some speculated it was a kind of Y2K-like problem, the most obvious cause seemed to be the overwhelming number of requests for tickets printed with the date and time 11/11/11 11:11. In the Japanese calendar, 1999 is written as Year 11, being the 11th year of the current emperor.

Dave Fossett, Saitama, JAPAN [via Andre Sintzoff]

🚨 Japan rail ticket system crash due to 11/11/11 11:11

Hiroshi Naito <mt5h-nitu@asahi-net.or.jp>

Sat, 13 Nov 1999 21:10:55 +0900

Newsgroups: misc.transport.rail.misc

The following is supplemental info of this incident.

The JR's ticket reservation and issuing system crashed on the day at around 11:11 because of intensive access caused by ticket collectors who were in favor of a string of 10 "1" letters (11, 11, 11, 11,11) printed on a platform ticket (Nyujo ken in Japanese). The first two digits indicate the year of Heisei 11 in original Japanese era

designation still in use as well as the year in the Christian calendar. Regular train tickets have time stamping printed up to date, but a platform ticket is printed up to minutes. At that time, the ticket collectors suddenly started purchasing platform tickets through the MARS system. The rate of platform tickets issued is usually only about three percent of the entire tickets while it reportedly soared up to 75 percent at 11:11 on the day. Besides, the system requires 150% more processing time per transaction for a platform ticket compared to for a regular train ticket. This situation caused a massive load on the central computer beyond its ticket issuing capability and resulted in the computer down.

This seems to be a good lesson as to the Y2K issue. The transport-related systems must be well verified and has been fixed for the date processing problem of Y2K, however, this incident suggests implication of system downs all over the world on 2000, 1, 1, caused by unexpected overwhelming transactions.

Hiroshi Naito [via Andre Sintzoff]

[I also received another take on this problem written by Nina Thorsen, sent via Martin Minow. PGN]

⚡ Computer prompts increase errors?

Ursula Martin <ursula@csl.sri.com>

Fri, 12 Nov 1999 18:49:43 -0800

<http://www.newscientist.com/ns/19991106/newsstory1.html>

This is a story about experiment suggesting more errors when relying on computer prompts than when reading instruments manually.

⚡ Re: Y2K creates "horseless carriages" (Doty, [RISKS-20.64](#))

Adam Elman <aelman@stanfordalumni.org>

Mon, 8 Nov 1999 21:44:52 -0800 (PST)

"Horseless carriage" is a legal designation used by some states to indicate a particular type of automobile registration, usually for early-20th-century cars. It's not an issue of a DMV programmer picking an odd-sounding category.

Of course, this points out a RISK of transient URLs; the San Jose Mercury usually leaves articles up only for a few days before they move them into their archive, where you have to pay to retrieve back content. However, I was able to find this article by searching on "horseless carriage" in both the San Jose Mercury News site and the Portland, ME Press-Herald (<http://www.portland.com/>) -- which makes it seem much less of an urban legend.

Adam [also noted by many other contributors! Thanks. PGN]

⚡ Possible risks in not examining end-user license agreements?

Anthony Garcia <agarcia@starbase.neosoft.com>

Thu, 18 Nov 1999 15:01:49 -0600 (CST)

Dialpad (www.dialpad.com) is a recently launched free net-to-telephone gateway service.

The marketing literature on their website states:

"Dialpad.com is the world's first free Java-based web-to-phone service. With Dialpad.com, you can make unlimited free phone calls to anybody in the US as long as the other party has a valid phone number."

and

"There is absolutely no cost involved in using Dialpad.com. The per call cost of Internet telephony is much lower than that of regular telephony. We bear the costs of calls you make and cover them with the revenue generated from banner ads."

To use the service, you have to download a Java applet that runs on your machine. Downloading the Dialpad client program requires that you click an "I Accept" button at the bottom of a web page containing their End User License Agreement, at http://www.dialpad.com/license_agreement.html

The Dialpad EULA starts off by identifying "The Dialpad.com Website" as "(the "Website" or "Site")" and continues off into the usual sort of EULA verbiage.

However, about halfway thru, it includes an interesting clause I've never noticed before on any other EULA:

Dialpad.com cannot and does not guarantee or warrant that the files available for downloading from the Site will be free of infection or

viruses, worms, trojan horses or other code that manifest
contaminating
or destructive properties. You are responsible for implementing
sufficient procedures and checkpoints to satisfy your
particular
requirements for accuracy of data input and output, and for
maintaining
a means external to the Site for the reconstruction of any lost
data. YOU ASSUME TOTAL RESPONSIBILITY AND RISK FOR YOUR USE OF
THE SITE,
SOFTWARE, SERVICE AND THE INTERNET.

It seems rather strange for Dialpad to make this disclaimer about
their own software's behavior.

Should we beware of Greeks bearing gifts, in this case? Can
such a clause
in an agreed-to EULA successfully indemnify someone who installs
a Trojan
Horse program on your machine, allowing them to claim your
consent?

Anthony Garcia <agarcia@neosoft.com>

Microsoft Y2K liability

Lloyd Wood <L.Wood@surrey.ac.uk>
Tue, 16 Nov 1999 15:56:29 +0000 (GMT)

I didn't know I was a Microsoft (UK) customer. Must be because
they
own Apple. And I refuse to take seriously any Y2K statement
ending with:

MOREOVER, MICROSOFT DOES NOT WARRANT OR MAKE ANY
REPRESENTATIONS

REGARDING THE USE OR THE RESULTS OF THE USE OF ANY MICROSOFT
YEAR

2000 STATEMENT IN TERMS OF ITS CORRECTNESS, ACCURACY,
RELIABILITY,

OR OTHERWISE.

disclaiming everything previously said, and sent by some clueless organisation that can't wrap to less than 80 chars.

<L.Wood@surrey.ac.uk>PGP<<http://www.ee.surrey.ac.uk/Personal/L.Wood/>>

[Get the full message from Lloyd if you are curious. PGN]

⚡ Risks of Office 2000

Lloyd Wood <L.Wood@surrey.ac.uk>
Wed, 17 Nov 1999 19:24:52 +0000 (GMT)

(Pointed out to me by Adam Kirby.) Try this in Office 2000.

Open a new document.
Type 'Hello World'.
Save as HTML.
View source of the saved document.

The length of the resulting document (three pages!) firmly places this in the 'extend' part of 'embrace and extend'. Risk? We're going to be drowning networks in even more redundant crud.

<L.Wood@surrey.ac.uk>PGP<<http://www.ee.surrey.ac.uk/Personal/L.Wood/>>

⚡ Re: Sarah Flannery ([RISKS-20.16](#))

Jean-Jacques Quisquater <jjq@dice.ucl.ac.be>
Thu, 11 Nov 1999 19:02:56 +0100

Do you remember Sarah Flannery and her new cryptoalgorithm?
Here are some links:

<http://jya.com/flannery.htm>

<http://www.intel.com/pressroom/archive/backgrnd/co51198a.HTM>

(including Gordon Moore and George Bush!)

<http://www.girlscientist.org/links.html>

See also comp.[risks 20.16](#) (15 J. 99)

Subject: 16-yr-old Irish girl's crypto system

With comments by PGN

The story continues:

<http://www.esat.ie/youngscientists/new/students/eu.htm>

http://www.cordis.lu/improving/src/hp_ys.htm

<http://europa.eu.int/comm/dg12/press/1999/pr2509en.html>

http://europa.eu.int/comm/dg12/press/1999/pr2509en_ann.pdf

And the paper

<http://cryptome.org/flannery-cp.htm>

Thanks to John Young.

✶ Slashes in spreadsheets (Re: [RISKS-20.64](#))

Kent Quirk <kent_quirk@cognitoy.com>

Sun, 07 Nov 1999 17:38:33 -0500

> From: Vicky Larmour <vicky.larmour@camcon.co.uk>

> ...why should forward slash be treated as an ALT press, but
> not if I

> am already editing text in a cell?

Ah, bitten by "ancient" history.

See, back in the days when Lotus was King and Microsoft a

wannabe, Lotus

1-2-3 was effectively an operating system on a lot of computers. There were huge numbers of people who started it up in the morning and used it all day long for everything -- not just spreadsheets, but letters, graphics, etc.

1-2-3's menu system (before any attempt at GUI standards and before the mouse was common) was invoked by hitting slash. Once you got used to it, you really really liked it. So /fr was "menu file retrieve", etc.

Lotus was forced by its customers to support this mode of usage in future spreadsheets. It did so by popping up a little dialog box containing nothing but the original 1-2-3 menu when you hit the slash key; whatever command you typed would then be translated to Windows GUI commands for you. (During the internal development process of the Windows version of 1-2-3, when this feature was introduced, the dialog box was labeled "Same as it ever was.")

Microsoft was busy watching the Lotus look-and-feel lawsuit around this time, and they presumably didn't wish to be **quite** as obvious as popping up a 1-2-3 menu system. So instead, they made the slash key invoke the windows menu in the same way that Alt does.

> Why isn't this listed in the keyboard shortcuts in the Excel help?

Probably because they had hopes of making it go away someday, and they didn't want to create a generation of users that depended on it.

Kent Quirk, Game Designer, kent_quirk@cognitoy.com <http://www.cognitoy.com/>

⚡ DVD crypto was intended to be weak

<mseecof@seatimes.com>

Tue, 09 Nov 1999 15:11:00 -0800

Sure, the DVD CCS encryption scheme was weak. Weak methods are cheap and easy to implement. Since people analyzing licensed software decoders would've broken even strong encryption of DVD movies, movie vendors had no incentive to pay for anything but weak encryption. They prefer to fight piracy with jackbooted enforcement of ill-conceived laws like the "Digital Millennium Copyright Act," an interesting Herman-Kahn'ian case of relying on deterrence rather than defence.

⚡ Amazon password change requests poorly authenticated

"Andrew R. Thomas-Cramer" <artc@prism-cs.com>

Mon, 15 Nov 1999 11:37:28 -0600

The Web business Amazon.com will provide new account passwords over the phone given only heavily-distributed public knowledge. Access to the account allows ordering with its credit-card number.

Because I'd forgotten my Amazon password, I called via voice to change it.

I was asked first for:

* My e-mail address.

- * The last purchase.

Since I didn't recall my last purchase, I was asked instead for:

- * My e-mail address.
- * My name.
- * My zip code.
- * The last four digits of my phone number.

I think it's in the realm of possibility that one or two other people might know my e-mail address, name, zip code, and phone number. I haven't yet received an e-mail notice that my password has changed, but it's been only ten minutes.

Fortunately, the shipping address for an order can't be changed unless the credit card number is re-entered. However, this only reduces, not eliminates, the risk of theft, and it doesn't forestall pranks.

BTW, this e-mail was **not** sent from the same address referenced by my Amazon account.

⚡ Who protects me from the protectors?

<David Mediavilla>

Tue, 9 Nov 1999 14:32:46 +0100

The Agencia de Protección de Datos (<http://www.ag-protecciondatos.es/>) is the Spanish authority that registers and oversees use of personal data (names, addresses,...) in private and official files.

They offer a form (<http://www.ag-protecciondatos.es/dato4.htm>) for requests from citizens.

The form redirects to a ~secure~ server
<https://wwws.servicom.es/ag-protecciondatos/dato4.htm> .
There, you must (according to standard procedure
https://wwws.servicom.es/ag-protecciondatos/por_que.htm)
provide your
personal data (name, postal address, e-mail address).

It is the first time an official organization requests my postal
address and
e-mail address at the same time. But I may think that since
these people are
the ones who defend me against privacy breaches, they will keep
my privacy.

All this trust is lost because, in the jump to secure HTTP, they
used an SSL
2.0 certificate from RSA Data Security valid until _12/10/99_
23:59:59.

David Mediavilla Ezquibela <davidme.forum@bigfootNOSPAM.com>

⚡ Risks of advertisements in software

"Bill Royds" <broyds@home.com>
Sun, 14 Nov 1999 22:51:27 -0500

A company called Conducent (<http://www.conducent.com> also called
TimeSink)
is offering to pay creators of free Microsoft Windows software
if the
software contains modules to display banner ads when the
software is
used. These modules are installed on the client's machine when
the freeware
is installed and is added to the user's start-up entry in the
Windows
Registry file without informing the user of the fact. This is an
entry for
TSADBOT.exe in the

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run entry. Shareware the does this includes PKZipW and Cute-FTP.

When the user runs the software, an Internet connection is attempted to a bank of computers controlled by Conducent, posting information about what program is running and other information about the user. This seems to be the method by which Conducent determines which software is running for royalty payments. It also uses the information to determine which advertising to show the user.

This is very similar to the Trojan horses that worry people so much and is probably illegal in countries with strong privacy laws. If someone was able to intercept these transmissions they could determine internal network and personal information about a user. Many users would not install these programs if the realised the nature of how the advertising works.

But an even worse fate occurs if the AdBot is thwarted in its attempts to connect to Conducent by a firewall or other controls. It starts to attempt to connect continually, about 10 times/second causing a huge load on local network facilities. If it can't connect even then, it tries to connect using Telnet and other ports with the background AdBot retrying the HTTP connects after several hours.

Bill Royds, 3414 McCarthy Road, Ottawa, ON K1V 9A1 Canada
1-513-733-7727 BRoyds@home.com

Workshop on Freedom and Privacy By Design

Lorrie Cranor <lorrie@RESEARCH.ATT.COM>

Fri, 12 Nov 1999 17:30:33 -0500

(Note the extended deadline)

DEADLINE REMINDER, CALL FOR PARTICIPATION
WORKSHOP ON FREEDOM AND PRIVACY BY DESIGN

COMPUTERS, FREEDOM, AND PRIVACY 2000

--> Submissions due November 30, 1999 <--

Westin Harbor Castle Hotel, Toronto, Canada, 4-7 April 2000

<http://www.cfp2000.org/>

This announcement is at <http://www.cfp2000.org/workshop>

PURPOSE:

CFP has traditionally focused strongly on legal remedies as essential instruments in the fight to ensure freedom and privacy. But law is often very slow to catch up to technology, and has limited reach when considering the global scope of modern communication and information technologies.

This workshop instead explores using -technology- to bring about strong protections of civil liberties which are guaranteed by the technology itself---in short, to get hackers, system architects, and implementors strongly involved in CFP and its goals. Our exploration of technology includes (a) implemented, fielded systems, and (b) what principles and architectures should be developed, including which open problems must be solved, to implement and field novel systems that can be inherently protective of civil liberties.

We aim to bring together implementors and those who have studied the social issues of freedom and privacy in one room, to answer questions such as:

- o Implementation
 - o How can we avoid having to trade off privacy for utility?
 - o What sorts of tools do we have available?
 - o What sorts of applications may be satisfied by which architectures?
 - o What still needs to be discovered?
 - o What still needs to be implemented?
 - o Is open source software inherently more likely to protect civil liberties, or not? Should we push for its wider adoption?
- o Motivation
 - o How do we motivate businesses to field systems that are inherently protective of their users' civil liberties---even or especially when this deprives businesses of commercially-valuable demographic data?
 - o How can we encourage users to demand that implementors protect users' rights?
- o Evaluation criteria
 - o Given some particular goal(s) for a particular project or technology--- such as protecting privacy---can we tell in advance if the end result is likely to help?
 - o How can we tell if a system, once fielded, has achieved its goal(s)?

The intended end products of this workshop are:

- o Ideas for systems that we should field, and
- o Implementation strategies for fielding them.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 66

Weds 1 December 1999

Contents

- [ATM User Trapped for 9 Hours](#)
[Jack Burke](#)
- [Dell loses five days' production time to FunLove Virus](#)
[Mich Kabay](#)
- [Risk of portable signs](#)
[Geoff Speare](#)
- [Irish telephone network outage brings Y2K fears](#)
[Dermot Casey](#)
- [Firestation fire blamed on Y2K computer fix](#)
[Kevin Whelan](#)
- [Halifax suspends net share dealing over security flaw](#)
[Nigel Cole](#)
- [Hacker links Staples to online rival Office Depot](#)
[Mich Kabay](#)
- [Risks of "anonymous" e-mail accounts](#)
[Bruce Schneier](#)
- [Sticky fingers with e-mail](#)
[Peter Wayner](#)
- [Privacy breach + plaintext passwords + denial of service](#)
[David Mediavilla](#)

- [Netscape 4.7 Danger: "Active" Newsgroup Messages](#)
[John David Galt](#)
 - [Expanding, Embracing, Devouring: IE 5.0 Task Scheduler Elevates](#)
[RA Downes](#)
 - [No bounds checking in Microsoft RTF controls](#)
[RA Downes](#)
 - [More on DVD encryption cracked](#)
[Bruce Schneier](#)
 - [Computer virus tears through companies](#)
[Dave Farber](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ ATM User Trapped for 9 Hours

Jack Burke <jfb3@mindspring.com>

Sun, 28 Nov 1999 12:40:10 -0500

Talk about poor planning by a New Jersey bank--I can't believe that no one thought of this situation.

The short version: a bank's inside-the-lobby ATM machine was being used by a man when the lobby's outside doors automatically locked at 9pm on Thanksgiving evening. There was no alarm button (apparently not even a fire alarm lever), no emergency exit, and no way out until the bank manager showed up the next morning (although I wonder why he didn't break the door or window to escape).

The man rightfully closed his account the next day.

http://www.apbnews.com/newscenter/breakingnews/1999/11/27/trapped1127_01.html

[Also noted by Daniel P. B. Smith]

⚡ Dell loses five days' production time to FunLove Virus

Mich Kabay <mkabay@compuserve.com>

Mon, 22 Nov 1999 13:48:50 -0500

Dell Computer's plant in Cork, [*] Ireland suffered five days of downtime after the company discovered that 500 of its computers had been infected with the FunLove virus. Staff had to track down the source of the infection and eradicate the virus from all its systems. Paul Taylor (Reuters) wrote, "the attack is regarded as one of the most damaging seen in Europe." In addition to the lost production time, the incident damaged customer relations, with some customers complaining about the delay in delivery of their systems.

M. E. Kabay, PhD, CISSP / Director of Education
R&D Group, ICSA Labs <<http://www.icsa.net>>

[Subsequent added note: Limerick City, not Cork? PGN]

⚡ Risk of portable signs

Geoff Speare <geoff@igcn.com>

Mon, 22 Nov 1999 09:45:20 -0500

The highway I use in my commute to work has been under construction for several months. The construction people were kind enough to park

a portable
sign unit (LCD display, 3 lines of 8 chars, readable from the
car) a couple
miles before the construction site. Normally, this sign warns of
things
like blasting, change in traffic patterns, etc. However, this
morning, the
sign read:

BATTERYS
NEED
CHARGING

The risk? That a generation will grow up thinking that
"batteries" is
spelled with a Y...

Geoff Speare <geoff@igcn.com>

Irish telephone network outage brings Y2K fears

"Casey, Dermot (CAP, GCF)" <Dermot.Casey@gecapital.com>

Tue, 23 Nov 1999 09:25:57 +0100

To summarise Eircom Ireland main teleco had a major failure last
Friday
afternoon. An upgrade which took place either Thursday night or
Friday
morning failed. When they switched to backup systems these also
failure due
to some embedded "software bugs" as described on the radio. The
collapse of
the first exchange caused a domino effect on exchanges in the
centre of
Dublin and businesses were left without a service from about
2.30 p.m to
6.00 p.m. Some 80,000 land-lines were effected initially, but
this rose
significantly as other exchanges were hit. People making calls
to numbers in

the affected areas were unable to reach them. To compound the problem Eircoms Cell phone customers in the same area were left without service due to an independent problem. The country's other mobile network Esat was unaffected. A few interesting points, why do people insist on upgrading during the working week when the risks are obvious. The second is this was Eircoms first big test for disaster recovery and it didn't come out very well. The Irish Telecoms Users Group has questioned Eircoms Y2K preparedness based on this incident. An Eircom spokesperson said that they were Y2K ready (£ 25 million project, 70 dedicated staff over a number of years) but admitted there were likely to be "glitches" in the system. see the Irish Times Archive for text of a story covering the incident. <http://www.ireland.com/scripts/search/highlight.plx?TextRes=eircom&Path=/newspaper/finance/1999/1120/fin50.htm>

🔥 Firestation fire blamed on Y2K computer fix

Kev <kwhelan@gamma.aei.ca>

Mon, 22 Nov 1999 00:59:04 -0500

This past Tuesday's *Montreal Gazette* reports a fire that caused \$500,000 damage to a local fire station. The fire started when one of the firemen left french fries cooking when responding to an alarm. The breaker system designed to cut off power to the stove when this occurs had been disconnected ... because it was incompatible with the new Y2K compatible

computer system recently installed!!!

In addition to the irony of a fire destroying the fire station and a safety system being disconnected because it's incompatible to the new computer system, the station had recently been the object of a successful community effort to save the historic old building from destruction during a development project.

According to a city official a patch is required to make the power cut off system compatible with the new system. No details were given regarding the hardware or software for either the new Y2K system or the power cut off system.

Ah, the risks of avoiding risks!

Kevin Whelan <kwhelan@mail.aei.ca>

✶ Halifax suspends net share dealing over security flaw

Nigel Cole <postmaster@zebekia.demon.co.uk>

Fri, 26 Nov 1999 20:33:54 +0000

I originally caught this on CEEFAX teletext service in the UK, but (naturally) it's also on the web:

http://news.bbc.co.uk/hi/english/business/newsid_538000/538285.stm

Summary: The Halifax (a UK bank) has suspended its online share dealing service after a serious security flaw was found. The flaw made it

possible for customers to not only see other customers' accounts, but also to buy and sell shares from them.

Dr. Nigel Cole postmaster@zebekia.demon.co.uk

[also noted by David Stringer-Calvert in the *Yorkshire Evening Press*,
27 Nov 1999]

⚡ Hacker links Staples to online rival Office Depot

Mich Kabay <mkabay@compuserve.com>

Tue, 30 Nov 1999 12:51:32 -0500

On 9 Oct 1999, someone breached security on the Staples Web site and redirected browsers to the Web site of Office Depot, the victim's major competitor. On 30 Nov 1999, Staples announced on that it filed a federal "John Doe" lawsuit against its assailant(s) claiming damages for lost business and for the recovery effort. Staples and Office Depot both said they doubted that Office Depot was in any way responsible for the attack.

M. E. Kabay, PhD, CISSP / Director of Education
R&D Group, ICSA Labs <<http://www.icsa.net>>

⚡ Risks of "anonymous" e-mail accounts

Bruce Schneier <schneier@counterpane.com>

Tue, 30 Nov 1999 15:20:17 -0600

Someone sent a bomb threat from an account from an account named shadowmega@hotmail.com. The police contacted Hotmail, and found that the Hotmail account had been accessed at a particular date and time, using an IP address owned by America Online. Using the AOL information, police identified exactly who was using that IP address at that time and were able to trace the sender to his apartment in Brooklyn.

Full story:

<http://www.zdnet.com/zdtv/cybercrime/news/story/0,3700,2324068,00.html>

Moral: Don't assume that your anonymous e-mail account is anonymous.

Bruce Schneier, CTO, Counterpane Internet Security, Inc. Ph: 612-823-1098
3031 Tisch Way, 100 Plaza East, San Jose, CA 95128 Fax: 612-823-1590

Sticky fingers with e-mail

Peter Wayner <pcw@flyzone.com>

Tue, 23 Nov 1999 07:51:52 -0500

According to the AP, a company which acted both as an ISP and a bookseller would use its position in the chain of e-mail to intercept e-mail messages between Amazon and customers who had accounts at the ISP. The ISP apparently used the information to try to gain a competitive advantage as it entered the business. New management settled for a fine of \$250,000. There was no mention if the ISP maintained the ability to turn its rack of

servers into
40-bit crypto crackers.

✶ Privacy breach + plaintext passwords + denial of service

<David Mediavilla>

Wed, 1 Dec 1999 19:42:23 +0100

I left my resume at JobUniverse <http://www.idg.es/JobUniverse/curriculum.asp>,
a Spanish job search site. The site claims to keep personal data safe and to have registered with the Spanish Personal Data Agency (See my post on [RISKS-20.65 http://catless.ncl.ac.uk/Risks/20.65.html#subj15](http://catless.ncl.ac.uk/Risks/20.65.html#subj15))

On 30 Nov 1999, I received e-mail reminding me of updating the resume.

It was politely signed by some Javier Nieto, director of IDG.ES. It included my e-mail address and the password I used. This is a risk but not very high.

The problem comes when they sent to some addresses (not all) another message including in To: field lots of e-mail addresses (I printed one and it covers 4 pages). In the body, the reminder text including the e-mail address and password of lots of subscribers. I haven't counted them but the message weighs 170-190 KB (57 pages). And better, they sent this message several times. I received 12, others 182 or 48 copies.

After several hours, they removed the resume service from the web.

So privacy breach + plaintext passwords + denial of service. I

haven't heard
about viruses... yet.

David Mediavilla Ezquibela <davidme.forum@bigfootNOSPAM.com>

⚡ Netscape 4.7 Danger: "Active" Newsgroup Messages

<John_David_Galt@acm.org>

Wed, 01 Dec 1999 13:11:15 -0800

Last night, I encountered the newsgroup spam message quoted in full below.

As soon as it is viewed, it causes my browser, Netscape Communicator 4.7, to load an unwanted web page -- even though I have preferences set to disable Java and JavaScript in news and mail messages. (The ">" I have added on each line disables this "feature.")

This behavior, of course, opens one's system to all the kinds of mischief a hostile web page can do, from giving spammers your e-mail address to running mischievous Java applets or viruses on your machine. Yet when I complained of this on Netscape's forum (the netscape.communicator newsgroup hosted at secnews.netscape.com), it was laughed off and they appear to have no intention of doing anything about it.

No browser has any business ever loading a URL unless the user requests it!

John David Galt

> Message-ID: <3841D1F1.C01EAA5D@softcom.net>
> Date: Sun, 28 Nov 1999 17:08:01 -0800
> From: "Jonathan H. Ballard" <cybertronix@softcom.net>
> Organization: Cybertronix

```
> X-Mailer: Mozilla 4.51 [en] (X11; I; FreeBSD 3.2-RELEASE i386)
> X-Accept-Language: en
> MIME-Version: 1.0
> Newsgroups: ca.test, ca.driving, ca.earthquakes, ca.
environment, ca.general
> Subject: HOPE
> Content-Type: text/html; charset=UTF-8
> Content-Transfer-Encoding: 7bit
> NNTP-Posting-Host: 209.160.172.191
> X-Trace: 30 Nov 1999 17:06:02 -0800, 209.160.172.191
> Lines: 12
> Path:
news-west.eli.net!sdd.hp.com!enews.sgi.com!news.idt.net!howland.
erols.net!newsfeed.fast.net!uunet!ffx.uu.net!news.sac.bfp.net!
209.160.172.191
> Xref: news-west.eli.net ca.test:900 ca.driving:6671 ca.
earthquakes:1464 ca.environment:3407 ca.general:17258
>
>
> --
> cybertronix@softcom.net jon.ballard@usa.net
> http://www.softcom.net/users/cybertronix
> Save a Tree -> Know How to eMail
> ;) CopyRight Ballard
```

⚡ Expanding, Embracing, Devouring: IE 5.0 Task Scheduler Elevates

<main@radsoft.net>

Tue, 30 Nov 1999 17:59:03 +0000

Re:

<http://www.ntsecurity.net/go/load.asp?id=/security/tasksched.htm>

What this article will demonstrate is that installing a web browser from Microsoft changes the topology of the underlying operating system - even

on Windows NT.

Ken Thompson used to say, "keep your hands off the drivers."
With all
the ridiculous crashes IE4 and IE5 have been guilty of, it's
obvious
Microsoft has never heeded that good advice.

Instead, they now muck about with the innards of your operating
system
when all they're really supposed to do is install a user mode
application.

The mind boggles.

RA Downes, Radsoft Laboratories <http://www.radsoft.net>

⚡ No bounds checking in Microsoft RTF controls

<main@radsoft.net>

Thu, 25 Nov 1999 14:08:50 +0000

I am speechless. Totally speechless. And for reasons which might
become
clearer later, I have a lump in my throat. This is not funny
anymore.
Dammit, it is not. I am mad.

The morning mailbox contained a newsletter on NT security, and
this
newsletter had an article about an attack on the Microsoft Rich
Edit
(RTF) controls. The URL given is:

[http://www.ntsecurity.net/go/load.asp?id=/security/richedit1.
htm](http://www.ntsecurity.net/go/load.asp?id=/security/richedit1.htm)

As there are a few discrepancies in the RTF code reproduced
there, I

made the mistake of assuming that this was a limited problem. But after disconnecting and thinking about the matter a bit (thinking still does have its advantages, even in this age when, thanks to Microsoft, information is at your fingertips) I realized it was "easy peasy" to crash any of Microsoft's Rich Edit (RTF) controls any time I wanted, and set about doing so.

But let's make sure everyone is up to speed before we continue.

RTF is a Microsoft invention (or so they claim) for formatting text. RTF stands for "Rich Text Format", thereof the description "Rich Edit" often used to describe this "technology". Microsoft encapsulates this "technology" all over the place, in their Office suite, in FrontPage, and in two resident system DLLs, RICED32.DLL and RICED20.DLL. Again, the attack works on any version of the DLL, and not just one or the other as the article at the above URL implies.

RTF consists of a number of "tokens" all introduced with the (you guessed it) backslash. An RTF file is always enclosed in braces (what good this does no one knows, next question please) and after the initial opening brace the token "\rtf1" should follow immediately. (The article online at the URL above incorrectly gives this token as "\rtf" - the '1' on the end, to the best of my knowledge, is necessary.)

As the article states, the buffer used for interpreting RTF tokens seems to be 36 bytes. This is such a ridiculous magic number it's not funny. I can't get past this one at all. The backslash is regarded as part of the

token in this context: thus any character sequence beginning with a backslash and continuing with at least 35 characters before the next token will send the control south.

Also, RTF tokens are considered to conform to the American alphabet: any non American alphabetic character in a token will in effect break the token and avoid the attack.

Another tidbit that might prove beneficial to readers: the initial MS Rich Edit control, Riched32.DLL, was written in C, the follow up, Riched20.DLL (sic) is written in C++, and Microsoft probably regards this latter DLL as a vast improvement, which it is not. But as this attack works on all generations of the control it can be concluded that the same brain dead code snippet is in effect here in all cases.

The buffer for parsing an RTF token is 36 bytes (including backslash character) - and no checks are used in the code to make sure the buffer does not overflow.

There is evidence in the disassembly of a character pointer being incremented with the postfix ++ operator - that the loop not check that this pointer is within bounds really and truly boggles the mind.

I can think of hundreds, thousands, hundreds of thousands of loops I have written and seen over the years, everyone of course having a bounds check built in. I mean, this is very basic programming, isn't it?

```
for (cp = buf; cp < buf + BUFSIZE; cp++)  
    /* * */
```

I mean, this is all really very elementary, isn't it? Tell me I'm wrong! Please, someone, anyone, tell me I'm wrong!!!!

I used to think so. But now that "Redmond RuleZ", who knows what goes anymore? The real pity is that in a week, as everyone becomes aware of this issue and what is behind it, that people will just end up accepting it. Crimenee!!!!

This RTF control in all its generations is one of the most used controls from the Microsoft arsenal. That this control be subject to the kindergarten programming practices of Redmond is more than at least this author can stomach.

This is absolutely horrendous. I feel literally physically sick. This is not funny any more.

RA Downes

PS. As this affects almost everyone using any kind of PC program anywhere, I guess I'll just have to devote the rest of this day to writing a wrapper to protect us. The idea is simple: send all references to RTF editors to the wrapper instead, which will first parse the file for evidence of malignant tokens, and then pass the file on to the target editor if all is in order - or otherwise issue a warning and drop the matter entirely. Drop me a line if you have any ideas. As Microsoft will probably handle this "issue" as so many others - i.e. ignore it - and as I rather trust my own code at this point far more than I trust Microsoft's (nil trust there to be honest) I think we have to

take
matters into our own hands.

RA Downes, Radsoft Laboratories <http://www.radsoft.net>

✶ More on DVD encryption cracked ([RISKS-20.64-65](#))

Bruce Schneier <schneier@counterpane.com>

Mon, 29 Nov 1999 21:58:40 -0600

The scheme to protect DVDs has been broken. There are now freeware programs on the net that remove the copy protection on DVDs, allowing them to be played, edited, and copied without restriction.

This should be no surprise to anyone, least of all to the entertainment industry.

The protection scheme is seriously flawed in several ways. Each DVD is encrypted with something called Content Scrambling System (CCS). It has a 40-bit key. (I have no idea why. The NSA and the FBI shouldn't care about DVD encryption. There aren't any encrypted terrorist movies they need to watch.) It's not even a very good algorithm. But even if the encryption were triple-DES, this scheme would be flawed.

Every DVD player, including hardware consoles that plug into your television and software players that you can download to your computer, has its own unique unlock key. (Actually, each has several. I don't know why.) This key is used to unlock the decryption key on each DVD. A DVD

has 400 copies of the same unique decryption key, each encrypted with every unlock code. Note the global secret: if you manage to get one unlock key for one player, you can decrypt every DVD.

But even if this were all perfect, the scheme could never work.

The flaw is in the security model. The software player eventually gets the decryption key, decrypts the DVD, and displays it on the screen. That decrypted DVD data is on the computer. It has to be; there's no other way to display it on the screen. No matter how good the encryption scheme is, the DVD data is available in plaintext to anyone who can write a computer program to take it.

And so is the decryption key. The computer has to decrypt the DVD. The decryption key has to be in the computer. So the decryption key is available, in the clear, to anyone who knows where to look. It's protected by an unlock key, but the reader has to unlock it.

The DVD software manufacturers were supposed to disguise the decryption program, and possibly the playing program, using some sort of software obfuscation techniques. These techniques have never worked for very long; they only seem to force hackers to spend a couple of extra weeks figuring out how the software works. I've written about this previously in relation to software copy protection; you can't obfuscate software.

It might be a bitter pill for the entertainment industry to swallow, but software content protection does not work. It cannot work. You

can
distribute encrypted content, but in order for it to be read,
viewed, or
listened to, it must be turned into plaintext. If it must be
turned into
plaintext, the computer must have a copy of the key and the
algorithm to
turn it into plaintext. A clever enough hacker with good enough
debugging
tools will always be able to reverse-engineer the algorithm, get
the key, or
just capture the plaintext after decryption. And he can write a
software
program that allows others to do it automatically. This cannot
be stopped.

If you assume secure hardware, the scheme works. (In fact, the
industry
wants to extend the system all the way to the monitor, and
eventually do the
decryption there.) The attack works because the hacker can run
a debugger
and other programming tools. If the decryption device and the
viewing
device (it must be both) is inside a tamperproof piece of
hardware, the
hacker is stuck. He can't reverse-engineer anything. But
tamperproof
hardware is largely a myth, so in reality this would just be
another barrier
that someone will eventually overcome. Digital content
protection just
doesn't work; ask anyone who tried software copy protection.

One more lesson and an observation.

The lesson: This is yet another example of an industry meeting
in secret and
designing a proprietary encryption algorithm and protocol that
ends up being
embarrassingly weak. I never understand why people don't use
open,
published, trusted encryption algorithms and protocols. They're

always
better.

The observation: The "solution" that the entertainment industry has been pushing for is to make reverse-engineering illegal. They managed in the United States: the Digital Millennium Copyright Act includes provisions to this effect, despite the protests of the scientific and civil rights communities. (Yes, you can go to jail for possessing a debugger.) They got a similar law passed in the UK. They're working on the EU. This "solution" does not work and makes no sense.

First, unless reverse-engineering is illegal everywhere on the planet, [and UCITA would like to do that; PGN] someone will be able to do it somewhere.

And one person is all you need; he can write software that everyone else uses. Second, the reverse-engineer can -- as in this case -- work anonymously. Laws wouldn't have helped in this case. And third, laws can't put the cat back into the bag. Even if you could catch and prosecute the hackers who did this, it wouldn't affect the hacker tools that have already been, and continue to be, written.

What the entertainment industry can do, and what they have done in this case, is use legal threats to slow the spread of these tools. So far the industry has threatened legal actions against people who have put these software tools on their Web sites. The result will be that these tools will exist on hacker Web sites, but will never be in public-domain software --

Linux, for example.

The fatal flaw is that the entertainment industry is lazy, and is attempting to find a technological solution to what is a legal problem. It is illegal to steal copyrights and trademarks, whether it is a DVD movie, a magazine image, a Ralph Lauren shirt, or a Louis Vitton handbag. This legal protection still exists, and is still strong. For some reason the entertainment industry has decided that it has a legal right to the protection of its technology, and that makes no sense.

Moreover, they are badgering legislatures into passing laws that prop up this flawed technological protection. In the US and UK (and possibly soon in the EU), it is illegal to circumvent their technology, even when you never use it to violate a copyright. It is illegal to engage in scientific research about the encryption used in these systems. It is illegal to peek under the hood of this thing you have legally bought. So not only does this system not work, it creates a black market where there was none before, while doing no social good in the process.

This DVD break is a good thing. It served no one's interests for the entertainment industry to put their faith in a bad security system. It is good research, illustrating how bad the encryption algorithm is and how poorly thought out the security model is. What is learned here can be applied to making future systems stronger.

<http://www.wired.com/news/technology/0,1282,32263,00.html>

<http://www.ntk.net/index.cgi?back=archive99/now1029.txt>

Summary of the DVD encryption scheme:

<http://crypto.gq.nu>

Geek stuff:

<http://livid.on.openprojects.net/pipermail/livid-dev/1999-October/000548.html>

<http://livid.on.openprojects.net/pipermail/livid-dev/1999-October/000589.html>

<http://livid.on.openprojects.net/pipermail/livid-dev/1999-October/000609.html>

<http://livid.on.openprojects.net/pipermail/livid-dev/1999-October/000671.html>

My essay on software copy protection:

<http://www.counterpane.com/crypto-gram-9811.html#copy>

My comments on the Digital Millennium Copyright Act:

<http://www.zdnet.com/pcweek/news/0622/22wipo.html>

New Intel software obfuscation techniques that, I predict, will be broken soon:

<http://www.intel.com/pressroom/archive/releases/in110999.htm>

(This originally appeared in the November issue of Crypto-Gram.

To subscribe, visit <http://www.counterpane.com/crypto-gram.html> or send a

blank message to crypto-gram-subscribe@chaparraltree.com.)

Bruce Schneier, CTO, Counterpane Internet Security, Inc. Ph: 612-823-1098

3031 Tisch Way, 100 Plaza East, San Jose, CA 95128 Fax: 612-823-1590

🔥 Computer virus tears through companies (From IP)

Dave Farber <farber@cis.upenn.edu>

Wed, 01 Dec 1999 04:42:58 -0500

Computer virus tears through companies

SAN FRANCISCO (AP) - A computer virus rampaged through corporate systems, devouring files, crippling e-mail systems and affecting thousands of computers Tuesday, according to anti-virus experts. The Mini-Zip virus, related to one that caused a serious outbreak in June, was expected to renew its assault Wednesday morning as unsuspecting users checked their e-mail inboxes. Sal Viveros, a marketing manager for Santa Clara-based Network Associates, which makes the McAfee anti-virus software, said some 20 large corporations had been affected by Tuesday evening. Dan Schrader, vice president of new technology at Trend Micro in Cupertino, said he fielded complaints of significant problems from four Fortune 500 companies and scores of smaller companies.

<http://www.infobeat.com/stories/cgi/story.cgi?id=2562345881-19a>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 67

Tuesday 7 December 1999

Contents

- [Crack in GSM cell-phone encryption scheme](#)
[NewsScan](#)
- [Medical errors kill tens of thousands annually, panel says](#)
[Keith A Rhodes](#)
- [Modern fire-alarm systems](#)
[Steven M. Bellovin](#)
- [Why Computers are Insecure](#)
[Bruce Schneier](#)
- [Jail for possessing a debugger? More on DVD encryption cracked](#)
[Daniel A. Graifer](#)
- [Quicken cannot roll back transactions, and even lacks an Undo feature](#)
[Tom Welsh](#)
- [Microsoft Works not saving spreadsheets](#)
[Shez](#)
- [Inadvertent attachments with MS Outlook 98](#)
[Jon Freivald](#)
- [Counterfeit Japanese coins and resulting risk...](#)
[John F. Opie](#)
- [Coppermine bug stops PC shipments](#)
[Sam Kasseman](#)

- [Jane's article on cyberterrorism hype](#)
[Martin Minow](#)
 - [Stock performance charts](#)
[Jeremy Epstein](#)
 - [Railtrack timetable server has Y2K problems?](#)
[Christopher St.John](#)
 - [Worm.Mypic: Will Y2K provide cover for worm/viruses?](#)
[Mich Kabay](#)
 - [Y2K compliance](#)
[Identity withheld](#)
 - [Re: Irish telephone network outage brings Y2K fears](#)
[Henry Spencer](#)
 - [Risks of US-Euro date conversion](#)
[Ben Hines](#)
 - [Re: Mars climate orbiter](#)
[Michael Detambel](#)
 - [Re: Sarah Flannery](#)
[Timothy A. McDaniel](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Crack in GSM cell-phone encryption scheme

"NewsScan" <newsscan@newsscan.com>

Tue, 07 Dec 1999 07:11:00 -0700

Researchers Alex Birykov and Adi Shamir of Weizmann Institute in Israel have cracked the A5/1 encryption scheme that protects communications made over wireless phones using the GSM standard. The GSM protocol is employed in more than 215 million digital phones worldwide, including ones made by Pacific Bell and Omnipoint. Calling the researchers' claim "ridiculous," an Omnipoint executive says, "What they're describing is an academic exercise

that would never work in the real world. What's more, it doesn't take into account the fact that GSM calls shift frequency continually, so even if they broke into a call, a second later it would shift to another frequency, and they'd lose it." But UC-Berkeley computer security expert David Wagner believes that the discovery is "a big deal" that puts calls "within the reach of corporate espionage." (Source: *The New York Times*, 7 Dec 1999, <http://www.nytimes.com/library/tech/99/12/biztech/articles/07code.html>; from NewsScan Daily, 7 Dec 1999, reprinted with permission)

✦ Medical errors kill tens of thousands annually, panel says

"Keith A Rhodes" <rhodesk.aimd@gao.gov>
Wed, 01 Dec 1999 07:57:08 -0500

[NOTE: The privacy issues surrounding this new center will be massive. I believe it will be a real test of the government's will to apply the necessary resources to protect patient privacy. The IOM news release is at <http://www4.nationalacademies.org/news.nsf/isbn/0309068371?OpenDocument> and the purchase information is at <http://books.nap.edu/catalog/9728.html>]

More people die each year in the United States from medical errors than from highway accidents, breast cancer or AIDS, according to a report of a National Academy of Sciences' Institute of Medicine panel. Between 44,000 and 98,000 people die per year because of mistakes by medical

professionals
(and that is "probably an underestimate" because of unreported errors
and uncovered areas of care). [Source: CNN, 30 Nov 1999]

⚡ Modern fire-alarm systems

"Steven M. Bellovin" <smb@research.att.com>
Wed, 01 Dec 1999 21:43:49 -0500

The following note was sent to all occupants of my building:

> Today at 9:35 AM we experienced a Fire Alarm system failure.
You may have
> heard the bells or saw lights going off in certain parts of
the building.
> The program that controls the different parts of the alarm
system appeared
> to fail. We have completed repairs to the system and will
have a system
> programmer here tonight to perform testing.

A systems programmer to fix a fire alarm? Sigh.

⚡ Why Computers are Insecure

Bruce Schneier <schneier@counterpane.com>
Mon, 29 Nov 1999 10:30:20 -0600

Almost every week the computer press covers another security
flaw: a virus
that exploits Microsoft Office, a vulnerability in Windows or
UNIX, a Java
problem, a security hole in a major Web site, an attack against
a popular
firewall. Why can't vendors get this right, we wonder? When

will it get
better?

I don't believe it ever will. Here's why:

Security engineering is different from any other type of engineering. Most products, such as word processors or cellular phones, are useful for what they do. Security products, or security features within products, are useful precisely because of what they don't allow to be done. Most engineering involves making things work. Think of the original definition of a hacker: someone who figured things out and made something cool happen. Security engineering involves making things not happen. It involves figuring out how things fail, and then preventing those failures.

In many ways this is similar to safety engineering. Safety is another engineering requirement that isn't simply a "feature." But safety engineering involves making sure things do not fail in the presence of random faults: it's about programming Murphy's computer, if you will. Security engineering involves making sure things do not fail in the presence of an intelligent and malicious adversary who forces faults at precisely the worst time and in precisely the worst way. Security engineering involves programming Satan's computer.

And Satan's computer is hard to test.

Virtually all software is developed using a "try-and-fix" methodology.

Small pieces are implemented, tested, fixed, and tested again.

Several of these small pieces are combined into a module, and this module is then tested, fixed, and tested again. Small modules are then combined into larger modules, and so on. The end result is software that more or less functions as expected, although in complex systems bugs always slip through.

This try-and-fix methodology just doesn't work for testing security. No amount of functional testing can ever uncover a security flaw, so the testing process won't catch anything. Remember that security has nothing to do with functionality. If you have an encrypted phone, you can test it. You can make and receive calls. You can try, and fail, to eavesdrop. But you have no idea if the phone is secure or not.

The only reasonable way to "test" security is to perform security reviews. This is an expensive, time-consuming, manual process. It's not enough to look at the security protocols and the encryption algorithms. A review must cover specification, design, implementation, source code, operations, and so forth. And just as functional testing cannot prove the absence of bugs, a security review cannot show that the product is in fact secure.

It gets worse. A security review of version 1.0 says little about the security of version 1.1. A security review of a software product in isolation does not necessarily apply to the same product in an operational environment. And the more complex the system is, the harder a security evaluation becomes and the more security bugs there will be.

Suppose a software product is developed without any functional testing at all. No alpha or beta testing. Write the code, compile it, and ship. The odds of this program working at all -- let alone being bug-free -- are zero. As the complexity of the product increases, so will the number of bugs. Everyone knows testing is essential.

Unfortunately, this is the current state of practice in security. Products are being shipped without any, or with minimal, security testing. I am not surprised that security bugs show up again and again. I can't believe anyone expects otherwise.

Even worse, products are getting more complex every year: larger operating systems, more features, more interactions between different programs on the Internet. Windows NT has been around for a few years, and security bugs are still being discovered. Expect many times more bugs in Windows 2000; the code is significantly larger. Expect the same thing to hold true for every other piece of software.

This won't change. Computer usage, the Internet, convergence, are all happening at an ever-increasing pace. Systems are getting more complex, and necessarily more insecure, faster than we can fix them -- and faster than we can learn how to fix them.

Acknowledgements: The phrase "programming Satan's computer" was originally Ross Anderson's. It's just too good not to use, though. A

shortened version of this essay originally appeared in the November 15 issue of Computerworld, and also in the November Crypto-Gram.

Bruce Schneier, CTO, Counterpane Internet Security, Inc. Ph: 612-823-1098

3031 Tisch Way, 100 Plaza East, San Jose, CA 95128 Fax: 612-823-1590

Free Internet security newsletter. See: <http://www.counterpane.com>

✶ Jail for possessing a debugger? More on DVD encryption cracked (20.66)

"Daniel A. Graifer" <dgraifer@cais.com>

Fri, 03 Dec 1999 13:54:39 -0500

By reading the law like programmers, we may be in danger of going off half-cocked. Let me illustrate by analogy:

I recently served on the jury for the trial of a man caught outside a health gym in possession of credit cards stolen from that gym both that day and earlier, and a switchblade knife and a set of filed keys. Among the charges he faced was "possession of burglarious tools". Burglarious Tools are implements used or intended to be used to commit a burglary. The intended use in this case was pretty clear: how else did he come into possession of the credit cards if he hadn't broken into the lockers they came from? Some implements help demonstrate intent by themselves: What else would you use filed keys for? His actions made the knife one

too; Even a screwdriver is a burglarious tool if that's what you are going to use it for. So yes, you CAN go to jail for possessing a screwdriver! Only an attorney could tell you if the new copyright protection laws are truly analogous. Anybody know an intellectual property lawyer willing to submit his comments?

We are also assuming that the intent of these encryption devices is to absolutely stop all piracy of the protected material. It's not; Not anymore than you expect the catch lock on the front of your house to impede a professional burglar. They are only intended to stop casual opportunism, and establish legally that the perp had to know he was making an unauthorized entry. We all make decisions about what level of security our wealth and neighborhood prudently require (catch lock, deadbolt or sophisticated alarm system). In some cases, legislation or case law has established a standard. In other cases, the standard is set contractually, ie. by your insurance company. Some lawyer has told the entertainment industry that prudence and due diligence requires the use of encryption serious enough to foil a casual pirate in order to maintain their copyright. They have failed at this by opting for security by obscurity and not employing the publicly reviewed techniques. Just like nobody in a U.S. urban area depends on a catch lock that can be defeated with a credit card. Prudence requires something stronger.

Daniel A. Graifer, Parker & Company 1-888-426-6548
<dgraifer@cais.com>

Andrew Davidson & Company, 520 Broadway, 8th FL, NY 10012, (212)

274-9075

✂ Quicken cannot roll back transactions, and even lacks an Undo feature

Tom Welsh <tom@draco.demon.co.uk>

Tue, 23 Nov 1999 12:18:18 +0000

Intuit's Quicken financial package, widely used by individuals and small businesses to keep track of their bank accounts, reflects a surprising set of design values. While adding countless user interface features and even Internet access over a series of releases, this program still denies users the fundamental ability to roll back transactions. It does not even have the "Undo" feature which, starting in word processors and text editors, has come to be expected in all well-written Windows applications.

When someone has been using Quicken for a number of years, the register for each bank account contains thousands of transactions. Each has a date associated with it. Unfortunately, Quicken's editing facilities are quirky to say the least, and it is quite easy when trying to change part of a date field to wind up with a date from an entirely different year. If someone is entering a string of transactions - perhaps copied from a pile of receipts - and typing ahead rapidly, an incorrect date may be overlooked. Once the return key has been struck to enter the transaction, however, Quicken provides no facilities whatsoever to cancel it, or even to find

it.

Consider a register that contains over 3,000 transactions covering a period of five years up to the present. A mistyped transaction may end up with a date sometime in 1995 or 1996. Finding it again - even if the error is recognised - is like looking for a needle in a haystack. But the register will be impossible to reconcile properly until that rogue entry is found and set right.

The solution is quite simple. First of all, Quicken should provide an "Undo" feature. Second, the user should be able to commit or roll back any number of transactions once they have been entered. This should extend to being able to Quit and lose all changes made during the session. (Staggeringly, this option does not currently exist). Third, Quicken should keep a log or journal of all transactions entered. This could be provided as an option, and the length of the log could be made user-adjustable.

Integrity features like these would outweigh any number of cosmetic user interface "enhancements", wizards, and multimedia gimmickry.

✶ Microsoft Works not saving spreadsheets

Shez <newsreply@nospam.demon.co.uk>

Fri, 3 Dec 1999 06:15:39 +0000

Microsoft Works v. 4.5a for Windows does not properly save spreadsheets when you give the Save command during work. Instead it leaves the

disk file open
until you either Close the file window or Exit the application.

Whether data is written to disk at all prior to the file being closed is unclear - Explorer shows it as being 0 KB and won't allow access as the file is still open. This problem does not affect Works database and word processor files, which are saved properly at once.

The Risk is that if the system hangs before you exit Works, you may lose all your spreadsheet data even though you have pressed "save" from time to time during the session.

Workarounds:

Either (a) close and re-open the spreadsheet each time you save it;
or (b) tick the "make backup" box; after this the spreadsheet will be saved properly if you issue the save command twice.

This bug was discovered by <bfriesen@my-deja.com>, and I have subsequently verified it for myself. It is not known at this point whether other versions of Microsoft Works are affected.

✶ Inadvertent attachments with MS Outlook 98

"Jon Freivald" <jon@freivald.org>
Thu, 25 Nov 1999 11:33:48 -0500

On two occasions now I have been the recipient of e-mail with attachments that were not meant to be sent to me.

The e-mail was intended for me, but the attachments were not.

On both occasions, the sender was using MS Outlook 98 and had sent the attachments to their intended recipients earlier the same day.

On both occasions the attachments were of highly sensitive nature. (One a strategic planning document and the other a detailed expense report.)

On going to their sent items folder, neither sender showed the attachments with the message to me, and could not find any other indication (other than my contacting them about the attachments) that the attachments had been sent to anyone but their intended recipients.

One of the senders is configured to use a POP server and sent a new message. The other is configured to use the same Exchange 5.5 server that I am, and did a reply to a message I had sent him. The only commonality I am able to establish between the two incidents is MS Outlook 98 being used as the mail client. When I get a few moments to breath, I'm going to try to make the event reproduceable.

Shall I even bother to say -- the risks are painfully obvious!

Jon Freivald -- jon@freivald.org -- <http://www.freivald.org/~jon>

⚡ Counterfeit Japanese coins and resulting risk...

"John F. Opie" <jfo@feri.de>

Mon, 29 Nov 1999 17:36:49 +0100

In today's issue (29 November 1999) of the *Nikkei Weekly* there was an item on a problem developing in Japan with the relatively new 500 yen coin. This coin was introduced to replace a 500 yen note and is relatively simplistic, ie there is no bicolored metals, no special edging etc. 500 yen was around \$4.80 on 29. November.

It turns out that this coin can be easily counterfeited using a 500 won (Korean currency) coin worth only 50 yen. This coin is virtually identical to the 500 yen coin, and only needs a couple of seconds under a grinder to remove a small amount of metal in order to make weights identical.

So what, you may ask? Well, coin machines in Japan are a tad more popular than they are elsewhere, and if you toss in one of these obviously adulterated and counterfeit coins, they accept them as if they were a 500 yen coin. But rather than choosing a product, the crooks in this case press for coin return and the machine returns a 500 yen coin.

That's right, it's first in, first out. The sorting mechanism does not hold the coins until the item is chosen, but rather assumes that no one is going to pass counterfeit coins and passes them into the general bin. The system then, when returning money, doesn't return the coins actually entered, but rather a generic coin from a general supply.

It's turning into a major nightmare for the coin-operated machinery industry, since you can run large amounts of these coins through machines in

a rather short time (they are, of course, pre-loaded with a set amount of cash in order to make change for large bills, and of course the 500 yen coin is popular for this reason...).

The lesson to comp.risks? Of course, that assumption that a coin is a coin.

A counterfeit coin returned (last in first out, or holding the coins in a holder until a purchase was actually made, ie caching the coins until use) to a crook is useless and there would not be a multi-million yen loss; by passing them through into a generic coin bin, opportunities for abuse were created that will require reequipping all coin-operated vending machinery with new sensors or other ways of validating coins, and of course the general aggregation when you make a legitimate purchase and the machine gives you a handful of worthless slugs as change...

John F. Opie, Senior Economist, Feri GmbH jfo@feri.de Harald Quandt Haus, Am Pilgerrain 17, Postfach 1454 D-61284 Bad Homburg vor der Hoehe

⚡ Coppermine bug stops PC shipments

Sam Kasseman EECE <usa1@Glue.umd.edu>
Thu, 2 Dec 1999 09:21:53 -0500 (EST)

Dell has stopped shipping its Optiplex GX110 corporate desktop because a bug in the high-end Pentium III Coppermine processors can prevent booting.

[ZDNet]

✚ Jane's article on cyberterrorism hype

Martin Minow <minow@pobox.com>

Wed, 01 Dec 1999 15:44:55 -0800

SlashDot <<http://www slashdot.org/>> references an article to be published in Jane's Intelligence Review on "Cyberterrorism Hype", posted at <<http://jir.janes.com/sample/jir0525.html>>. The article's author, Johan J Ingles-le Nobel, discussed the subject with SlashDot contributors.

✚ Stock performance charts

"Epstein, Jeremy" <Jeremy_Epstein@NAI.com>

Fri, 3 Dec 1999 05:56:22 -0800

The Washington Post business section 22 Nov 1999 included a corrected chart showing performance of recent Washington-area IPOs, with the following note:

"The stocks of companies that have gone back to Wall Street to sell shares in the last two years have not performed as badly as appeared [in the November 15 issue] ... which were based on inaccurate information in the Bloomberg News database. Bloomberg failed to adjust for stock splits in the post-offering performance calculations Bloomberg is aware of the flaw and plans to fix it. The corrected chart ... shows that 18 of 39 secondary issues were trading above their offering prices as of

November 12.

That's a 46 percent success rate, substantially better than the 33 percent cited in [the November 15 issue]."

For a company that makes its living selling financial data, this seems like

a rather substantial oversight for Bloomberg! GIGO rules again?

--Jeremy Epstein, NAI Labs

✶ Railtrack timetable server has Y2K problems?

"Christopher St.John" <chris.st.john@NO.san.SPAM.com.PLEASE>

Wed, 24 Nov 1999 18:16:17 -0000

The UK Rail Operating company, Railtrack, have an online timetable information system which collates timetables from the various train operators (see www.railtrack.co.uk)

Recently a suspicious warning has appeared on their timetable form:

```
=====
Please read this BEFORE you travel!
We have identified a problem with our online timetable service.
```

Currently the online timetable may return inaccurate results. Though most of the information returned by the online timetable is accurate, weekend journey information and journey information for travel between Christmas Eve and January 2nd may be inaccurate.

We have identified the cause of this problem and are working on a solution as a matter of the highest priority. A full and accurate service

will be
restored as soon as possible.

✶ Worm.Mypic: Will Y2K provide cover for worm/viruses?

Mich Kabay <mkabay@compuserve.com>

Sun, 5 Dec 1999 22:10:29 -0500

The upsurge in e-mail-enabled worms and viruses appears to be supporting the predictions of anti-virus experts who said that the Y2K transition would see a flurry of new viruses and variants that would contribute to confusion about the source of software problems following New Year's Day 2000.

Nancy Weil, writing in ComputerWorld

<<http://www.computerworld.com/home/news.nsf/all/9912035y2kworm>> ,

suggested that the Worm.Mypic (aka W32/Mypics.worm) demonstrates the kind of problem we are going to face in coming weeks. Worm.Mypic arrives as an executable attachment (Pics4You.exe with a length of 34,304 b). If executed, the program e-mails itself to the usual first 50 names in the MS-Outlook address list (and continues to try to do so at regular intervals). As soon as the date changes to 1 Jan 2000, the resident virus overwrites checksum data for the computer's BIOS, interfering with the boot sequence. The virus also attempts to format C: and D: drives.

As usual, everyone agrees that it is critically important to update virus-signature files even more frequently than usual as we

approach the new
year.

M. E. Kabay, PhD, CISSP / Director of Education
R&D Group, ICSA Labs <<http://www.icsa.net>>

✶ Y2K compliance

Identity withheld by request <>

Fri, 3 Dec 1999

The IEEE created a document (either a standard, a standard practice, or a guide), I forget which status it achieved in which Y2K compliance was originally defined, essentially, as "the software will work after the start of the millennium". It was pointed out that this was ridiculous since the software might not work beforehand and it shouldn't suddenly work afterwards. So the definition was changed to, essentially "the software will work as well after the millennium as it did before".

Increasingly, I am seeing organizations break all kinds of software now, in their mad scramble to apply Y2K fixes (well, they are called fixes). If I apply the definition, it is clear that they are ensuring Y2K compliance by the following strategy.

Start with a currently operational system that may (or may not) be Y2K compliant. Apply Y2K fixes so that the system becomes non-operational and now, by the IEEE definition they are guaranteed to be Y2K compliant.

The real risk, behind this the above is, of course, that many organizations (including those that should know better) have left it *far* too late to apply and test patches and are now scrambling to become Y2K compliant. Who knows what will be broken next or the vulnerabilities that are being opened up?

[Yes, we know, 2000 is not the beginning of the next "millennium". PGN]

⚡ Re: Irish telephone network outage brings Y2K fears (Casey, R-20.66)

Henry Spencer <henry@spsystems.net>
Thu, 2 Dec 1999 11:13:50 -0500 (EST)

It sounds like the problem may have manifested itself only when the system was under load (if it took from night/morning until midafternoon for it to really make a mess), in which case having the upgrade done on the weekend might not have been an improvement.

There is also a practical issue: it is often safer to make such changes at times when your full staff is at work, so that minor problems can be spotted and handled quickly. This inherently conflicts with wanting to keep major failures out of the way of the customers, so it unfortunately requires guessing how serious the problems are likely to be. Sometimes you guess wrong.

✦ Risks of US-Euro date conversion (Re: Ezquibela, [RISKS-20.65](#))

Ben Hines <bhines@san.rr.com>

Mon, 22 Nov 1999 00:38:29 -0700

>All this trust is lost because, in the jump to secure HTTP,
they used an SSL
>2.0 certificate from RSA Data Security valid until _12/10/99_
23:59:59.

Of course, here in the US, where RSA is based, "12/10/99" is
December
10th, 1999, so the key is still valid. You, being in Spain and
interpreted this as October 12, 1999.

-Ben bhines@san.rr.com <<http://members.tripod.com/~tunnels/>>

✦ Re: Mars climate orbiter

Michael Detambel <detambel@mail.bfw-oberhausen.de>

Mon, 22 Nov 1999 13:03:57 +0100

Approximately 15 years ago I worked in a project on a Krupp
process
computer. I developed the application software in the real time
programming
language PEARL, a colleague the system software (e.g. a mask
generator and
handler for the 25x80 character display terminals) in the system
language of
the computer, META-S. For the interprogram communication he has
provided a
call interface, over which the field entrys and the field
attributes could
be exchanged. For the set and reset of the field attributes
there was a

byte, whose bits were assigned to individual values. E. g. if bit was 1 on, the field on the display should flash, with bit 2 the Field should appear in reverse mode representation etc. However, that never works and we needed some time, until we had found the bug: In the programming language PEARL the bits are counted from left to right, with beginning by the value "1" (the most significant bit first), in the programming language META-S from right to left (with the first value zero)...

Michael Detambel (Translated by Babelfish)

✉ Re: Sarah Flannery (Quisquater, [RISKS-20.65](#))

Timothy A. McDaniel <tmcd@jump.net>
Mon, 22 Nov 1999 11:32:54 -0600 (CST)

Jean-Jacques Quisquater <jjq@dice.ucl.ac.be> gave a number of links giving further information about Sarah Flannery and her proposed cryptosystem. It should be mentioned (as M. Quisquater did not) that the last link, the one containing her paper, <http://cryptome.org/flannery-cp.htm> has an postscript showing that her public-key system can be broken and "there's no hint yet of a repair". So far as I can tell, none of the other links he provided, to press releases and further information and such, mention that either.

Tim McDaniel, tmcd@jump.net



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 68

Tuesday 14 December 1999

Contents

- [RST discovers defective crypto in Netscape mail password saver](#)
[Gary McGraw](#)
- [Canada Post has "electronic post" on line](#)
[Alan DeKok](#)
- [Sanity.com: buy now, pay never](#)
[David Shaw](#)
- [A Tale of Two Web Sites: Calling it secure doesn't make it so](#)
[Steven J. Zeil](#)
- [IDs in color copies and prints: confirmed](#)
[Lauren Weinstein](#)
- [BBC Censorship!](#)
[Peter McWilliams via Lindsay Marshall](#)
- [Melissa perpetrator faces five years in prison](#)
[NewsScan](#)
- [Oh, no! Y2K virus competitions](#)
[Ross Stewart via Peter de Jager](#)
- [Re: No bounds checking in Microsoft RTF controls](#)
[meeroh](#)
- [Slashes in spreadsheets](#)
[Christopher Warnock](#)

[David Empson](#)

● [Risk of APC Power Chute](#)

[Geoffrey Coram](#)

● [Risks of e-mail monitoring](#)

[Thomas Roessler](#)

● [Re: Counterfeit Japanese coins and resulting risk...](#)

[Henry Spencer](#)

● [Re: Ladbroke Grove](#)

[Mark Brader](#)

● [USENIX Security Symposium 2000 - A Call for Papers](#)

[Moun Chau](#)

● [Call for Papers - Safecomp 2000](#)

[Gemma Windt-Krose](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ RST discovers defective crypto in Netscape mail password saver

Gary McGraw <gem@rstcorp.com>

Mon, 13 Dec 1999 17:18:18 -0500

Because remembering your passwords is a pain (you do have more than one, don't you?), many programs are set up to remember them for you. Exactly how they do this is a risky business. Netscape didn't do it right. Beyond simply stealing e-mail passwords, our discovery provides a gateway to other accounts and systems since people generally use the same password everywhere. Netscape has been notified of the flaw.

The POP3 and IMAP protocols are often used to read e-mail on a home or office PC from a central mail server. As a convenience to the user, many programs offer to remember the user's password. When Netscape offers to

save your e-mail password, it is encrypted before being stored in the registry or preferences file on your computer.

Unfortunately, the encryption algorithm used by Netscape to scramble passwords is exceptionally weak. Tim Hollebeek, an RST Research Associate, and John Viega, a member of the RST Software Security Group, were able to deduce the algorithm after only eight hours of work. No reverse engineering of the software was involved. Instead, a few hundred carefully chosen passwords were analyzed using pencil and paper. The algorithm turns out to be a simple combination of XOR with a constant key and a substitution cipher weaker than those found in puzzle magazines. For more details, see <http://www.rstcorp.com/news/bad-crypto.html>

Once the cipher is known, recovering a POP3 or IMAP password stored on a machine is trivial. Any attacker with physical access to the victim's machine or the ability to run code on it can use our exploit. Additionally, passwords can be stolen from some versions of Netscape remotely using Javascript.

RST has created a working password snagging attack in the lab. A successful attack allows the bad guy to download and read a victim's e-mail from a remote machine. Since careful use of the hack would not leave too many obvious clues, a victim's e-mail could be snooped indefinitely. The only workaround is to turn off the ``remember password'' feature.

Though stealing mail alone is a very serious security/privacy

problem, more dangerous scenarios exist. The largest risk is that people use the same password for POP3 and other logins to remote machines (and maybe even their PGP passphrase). In particular, many people use IMAP or POP3 to access work related e-mail from home, and their mail password is also the login password they use at work. In fact, the login account and the mail account are often the same. Home computers are notoriously insecure and easy to penetrate. A malicious attacker can read the POP3 password stored on an insecure home computer (often over the net) and use it to log in to a more secure machine run by the victim's employer. The attacker can then take control of an account, read sensitive information, attack more privileged accounts, and set up remote monitoring systems inside a corporate network. Our exploit code could also be used as a payload in a much more insidious version of Melissa.

Quote of the day: ``We didn't do this with just a pencil and some paper. Lots of our notes are in pen. We didn't need to erase much.''
Tim Hollebeek
& John Viega

Other quote: ``This is another illustration of how bad closed, proprietary, cryptography is. What makes this vulnerability particularly nasty is that people tend to use the same passwords over and over again. If you can attack someone's mail server password, you're likely to also have their login password, PGP password, etc. Software security is important.''
Bruce Schneier

Gary McGraw, Ph.D., Vice President, Corporate Technology
Reliable Software Technologies <http://www.rstcorp.com>

✶ Canada Post has "electronic post" on line

Alan DeKok <aland@striker.ottawa.on.ca>

Tue, 30 Nov 1999 19:02:41 -0500

Canada Post has recently been announcing it's new on-line mail service, "epost", at <http://www.epost.ca/>. They claim it's a secure on-line service for handling mail and bills via the web, as if it's something new and unique.

Why would I need an on-line central post office if I can PGP encrypt/sign my messages, or use a corporations SSL-enabled web site to view and pay my bills?

In addition, they still fall into the standard security traps. Your "secure" e-mail is stored on their servers, where it is vulnerable to non-web based attacks. This is equivalent to having the paper version of the post office open and sort all of your mail for you.

Their security statement at

http://www.epost.ca/guided/english/why_2a.html

has the following wonderful quote:

If you are accessing your ELECTRONIC POST OFFICE BOX[tm] using a Web

browser, you do not need to worry about viruses since no data are

exchanged between the computer you are using and our system.

Umm... right. How many security related browser bugs have their been in the past year?

Alan DeKok

Sanity.com: buy now, pay never

David Shaw <David.Shaw@alcatel.com.au>

Tue, 30 Nov 1999 16:00:58 +1100

The following is a summary of an article found on page 101 of the *Sydney Morning Herald*, Saturday November 27, 1999.

Sanity.com's web-site, www.sanity.com.au, an online audio CD shop, was launched on October 18, 1999 with a significant flaw. It was possible to order CDs and not have to pay for them.

Reports of the flaw resulted in Internet users swamping the web-site, prompting an official to say "We're close to having a meltdown."

The problem with the site began with a design flaw which was originally contrived to make life easier for consumers. Customers are given the option of ordering a CD online but are not required to enter their credit card details online if they feel uncomfortable about security.

The intention is of course that these customers would phone, fax or e-mail their credit card details before receiving their goods. However,

the site does not tell consumers the phone numbers or e-mails to use to pass on credit card details.

Customers who omitted their credit card details soon discovered they received the CDs anyway. Invoices obtained by the *Herald* showed that the "payment by" field was left blank.

Global Fulfilment, a US-based company, which provides the technical, financial and ordering system for the site, denied any technical error, but did reveal that the Sanity.com website had not installed an automated credit card processing system in the first few weeks of operation.

Sanity.com has cut its relationship with Global Fulfilment for the technical design of the site, which will now be done on-site. Global Fulfilment will still provide coordination and fulfilment of CD orders.

Sanity.com's shares are set to debut on the Australian Stock Exchange (ASE) today (Tuesday November 30, 1999) after an AUD\$8.4m float of 14%. Sanity.com maintains it lost no substantial revenue due to the free CDs and is therefore under no obligation to file a prelisting disclosure to the ASE. Sanity.com has stated that the problem has been fixed and that no customer would be retrospectively billed for any free CDs.

David Shaw, Alcatel Australia Limited david.shaw@alcatel.com.au

[I eschewed any spelling corrector's suggestions of Fulfillment or Fulfilament. PGN]

✦ A Tale of Two Web Sites: Calling it secure doesn't make it so

<szeil@notesmail.cs.odu.edu>

Thu, 9 Dec 1999 13:19:59 -0500

My wife was recently engaging in some on-line Christmas shopping, and stopped short of placing orders with two merchants because the usual "secure site" icon was not being displayed on the web browser's status line (both the latest versions of Netscape and Internet Explorer flagged the pages as unsecured).

The first point of interest was that both sites featured prominent "This site is secure" assurances, with links to pages explaining that they use secure servers to protect credit card and other customer information.

A little investigation showed that the first site, <http://www.toysrus.com>, really was using a secure https server, but the secured page was appearing as a frame inside a larger page from an unsecure server, thus fooling both browsers into displaying the "unsecured" icon.

The second site, <http://www.thesportsauthority.com>, showed no signs at all of using any security mechanism despite their stated "Privacy and Security Policy". We sent a message to their customer service address complaining of this fact and asking if they would honor the sale prices advertised on their web site even if we were to call their toll-free number and

place the order
by telephone. Their response absolutely floored us:

"Thank you for writing to www.thesportsauthority.com.

We apologize for any problems you are having using our site and appreciate your concerns and criticism regarding security. Please try placing your order again, as there has been ongoing adjustments to the pages. All our orders in the online store are placed via the Internet, even if you were to call us." [remainder omitted]

In other words, whether you click or whether you call, your credit card number is going out over the net via plain-text!

So, one site that is secure masquerades as insecure. Another is truly insecure, whether you use it or not!

Steven J. Zeil
~zeil

<http://www.cs.odu.edu/>

Dept. of Computer Science Old Dominion University Norfolk, VA
23529

⚡ IDs in color copies and prints: confirmed

Lauren Weinstein <lauren@vortex.com>
Wed, 08 Dec 99 14:52:59 PST

Greetings. In my latest PRIVACY Forum Digest, I've presented a report confirming the fact (well known in the copier trade, but something of an urban legend for everyone else) that xerographic color copiers/printers include "steganographically" encoded IDs. Essentially, these IDs are encoded repeatedly as part of the

background "noise" in images, and cannot be decoded without knowledge of the proprietary algorithms involved.

The full report can be viewed at:

<http://www.vortex.com/privacy/priv.08.18>

In that report, I mentioned the possibility of such IDs being implemented within inexpensive, consumer-level equipment. This could include both copiers and such widely-used devices as inkjet printers. Those readers who might question this possibility might wish to take a look at:

<http://www.bep.treas.gov/countdeterrent.htm>

which is a Bureau of Engraving and Printing procurement offering dealing with precisely these issues.

--Lauren--

Lauren Weinstein

lauren@vortex.com

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

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

⚡ BBC Censorship!

<Lindsay.Marshall@newcastle.ac.uk>

Fri, 3 Dec 1999 13:11:54 +0000 (GMT)

This item was in rec.humor.funny. If you go to <http://www.bbc.co.uk/home/today/> and try the "E-mail a friend" button, you can verify that this indeed happens.

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

From: Peter McWilliams <petermcw@geocities.com>

Newsgroups: rec.humor.funny
Sent: Friday, December 03, 1999 3:30 AM
Subject: BBC Censorship!

> The BBC web pages have links which allow you to send web pages
to e-mail
> addresses and to include a text message.
>
> I just sent myself a page with the word Saturday in the body
of the
> message. It arrived with the word changed to Sa****ay!
>
> Hmmm. So I tried sending...
>
> >"I hope you still have your appetite for scraps of dickens
when I bump
> >into you in class in Scunthorpe, Essex on saturday"
>
> Yes! It replied...
>
> >"I hope you still have your appetite for s****s of dickens
when I ***p
> >into you in class in S****horpe, Es*** on sa****ay"
>
> Missed the t**, the a** and the d*** though. [* This line PGN-
ed]

> Peter Mc*****ams

> Selected by Jim Griffith. MAIL your joke to funny@netfunny.
com.
> Attribute the joke's source if at all possible. A Daemon will
auto-reply.
>
> Jokes ABOUT major current events should be sent to
topical@netfunny.com
> (i.e., jokes which won't be funny if not given immediate
attention.)
> Anything that is not a joke submission goes to funny-
request@netfunny.com
> For the full submission guidelines, see <http://www.netfunny.com/rhf/>
>

> This joke's link: <http://www.netfunny.com/rhf/jokes/99/Dec/censorship.html>

[* The other parts (of speech!) have been truncated in the name of Internet Decency. PGN-Petered out, I guess]

⚡ Melissa perpetrator faces five years in prison

"NewsScan" <newsscan@newsscan.com>

Thu, 09 Dec 1999 09:32:30 -0700

David L. Smith, the New Jersey computer programmer who has pleaded guilty to having created the Melissa virus that infected more than 100,000 computers worldwide and caused an estimated \$80 million in damages, is likely to face a sentence of five years in federal prison. Security expert and former prosecutor Mark D. Rasch says, "The federal government is trying to send a message that they take these kinds of Internet crimes very seriously. This is also a recognition that a single individual has the ability to cause tens of millions of dollars of damage." (*The New York Times*, 9 Dec 1999, <http://www.nytimes.com/>; NewsScan Daily, 9 Dec 1999)

⚡ Oh, no! Y2K virus competitions

Ross Stewart <ross@wilsonwhite.co.nz>

Wed, 08 Dec 1999 13:23:21 +1300

[Via: Peter de Jager <pdejager@year2000.com> (tel 1-905-792-8706)]

>X-Sender: ars@pop.wilsonwhite.co.nz

>To: y2k_group@year2000.co.nz

>

>I don't have a lot of patience nor tolerance for those who use their

>talents to try and stuff up my life nor those of my staff by developing

>ever more sophisticated and warped viruses. All it does is cause us grief

>and hinders us from finding good jobs for smarter, more honourable and

>usually more intelligent IT professionals.

>

>We have just received a warning from an anti-virus specialist (poacher

>turned gamekeeper ?) about some idiots in Holland who have established a

>competition for the best Y2K virus. The p[i?]rates involved have set up

>"game rules" with the only requirement being that each entry has to be a

>virus/trojan or backdoor, and preferably related to the Millennium Bug or

>the year 2000.

>

>Quoting (after editing) from the site :

>"The viruses that will be sent for the Y2K infection feast [sic] will be

>sent 4-5 days before the release to AV companies. The one that gets

>detected last will be the winner."

>

>Words fail me.

>

>I'm told there are almost 50,000 viruses floating around the world

>now. It's a real pain that some stupid ***** is going to further

>waste my time over Y2K, just when I don't need the hassle. I'm sure you

>don't either.

>

>What to do?

>

>We're disconnecting our e-mail servers from the WWW and setting up an e-mail

>service on a standalone PC. This standalone machine will do ALL e-mail

>downloads from real soon now until well after New Year. We'll keep that

>machine loaded to the gunwales with the latest anti-virus software and will

>endeavour to ensure that any virus outbreaks are thus contained.

>

>We strongly suggest you seriously consider doing the same.

>

>We'll pass CVs internally across to other "more sensitive" machines in .rtf

>format (using rtf avoids Word-type macro viruses).

>

>Remember also that the major anti-virus companies have all agreed to

>provide FREE 90-day versions of their software to cover this period. GET

>SOME !!! before 31 December via <http://www.year2000.co.nz/y2k8.htm#antivirus>

>

>Lastly, remember to pull the power cord/s out of the wall socket/s when you

>go home before New Year, a simple method of avoiding any possible surge

>damage to electronic equipment.

>

>Thinks : Wouldn't it be nice if we could have a quiet Y2K period ????

>

> A R (Ross) Stewart, Wilson White Group, Auckland, New Zealand

> ross@year2000.co.nz <http://www.year2000.co.nz/>

ross@wilsonwhite.co.nz

> ph: +64(9)307-3869 (posted at <http://www.year2000.co.nz/y2kema21.htm>)

⚡ Re: No bounds checking in Microsoft RTF controls (Downes, R-20.66)

meeroh <meeroh@MIT.EDU>

Wed, 01 Dec 1999 18:28:12 -0500

```
>I can think of hundreds, thousands, hundreds of thousands of
loops I
>have written and seen over the years, everyone of course having
a bounds
>check built in. I mean, this is very _basic_ programming, isn't
it?
> for (cp = buf; cp < buf + BUFSIZE; cp++)
>     /* * */
```

It may be worth pointing out that a more correct way of implementing this loop is

```
size_t size = BUFSIZE;
while (size-- > 0) {
    /* ... */
}
```

The original code fails in the subtle case when `buf + BUFSIZE` extends past the end of the address space. Note that the ANSI C guarantee that you should be able to compute the address of the first element beyond the end of a named array doesn't apply if `buf` is dynamically allocated.

This common idiom, while it's guaranteed to work if `buf` is a named array of characters, will fail if `buf` was dynamically allocated -- yet almost every programmer I've seen uses the same idiom for both cases.

(See *Writing Solid Code* by Steve Maguire, p 132.)

meeroh

PS. Yes, I do realize that in the context of a local buffer with hardcoded size, which was the topic of the original post, this idiom is okay.

meeroh@mit.edu | <<http://meeroh.mit.edu/meeroh/>> | MIT I/S Mac developer

⚡ Slashes in spreadsheets (Re: Quirk, [RISKS-20.64-65](#))

"Christopher Warnock" <cwarnock@rocs.com>

Mon, 22 Nov 1999 08:04:31 -0500

The "slash" usage in Excel can be changed quite easily to another character or to nothing at all, effectively being disabled. In Excel, under Tools/Options, select the "Transition" tab and you will see the text "Microsoft Excel menu or Help key:" and this will have a text box to the right of it containing a "/" character. In this text box, type the character that you wish to use for this function and then select the "OK" button. Leave this text box blank to disable the functionality.

Christopher Warnock, CCNA, Senior Network Architect
Resource One Computer Systems V: 614.228.8165 F: 614.241.5810

⚡ Slashes in spreadsheets (Re: Quirk, [RISKS-20.64-65](#))

David Empson <dempson@actrix.gen.nz>

Tue, 23 Nov 1999 01:21:57 +1300

> From: Kent Quirk <kent_quirk@cognitoy.com>
>
> [Lotus] 1-2-3's menu system (before any attempt at GUI
standards and
> before the mouse was common) was invoked by hitting slash.
Once you got
> used to it, you really really liked it. So /fr was "menu file
retrieve",

It is even older than that: the slash key was used in the same
manner by the
original spreadsheet program: VisiCalc running on an Apple II
(circa 1980).

David Empson <dempson@actrix.gen.nz>
Snail mail: P O Box 27-103, Wellington, New Zealand

Risk of APC Power Chute

<Geoffrey Coram>
Tue, 7 Dec 1999 18:19:28 -0500

I recently installed APC's Power Chute Plus for Win98/NT, which
allows
control of various features of their UPS devices. I was
surprised when I
started the program that it listed two possible devices, mine
and another
machine in my building.

It turns out that the default installation of PC+ sets up the
installation
directory as shared to everyone in your workgroup - perhaps a
fine idea for
corporate networks, but not the right idea for cable modems and
campus dorms
(my case). I don't want my neighbors to have the ability to
simulate a
power failure - with the loud warning beep - at 4 AM, or
otherwise mess with

the settings.

I happened to have file sharing turned off, so the properties of the directory were ignored. I was surprised that this was not mentioned during the install process, but instead buried in the help file. APC tells me they will consider my recommendation to switch the default, and let the (presumably) more knowledgeable corporate network administrator enable the feature if he wants it.

Just another risk of shared networks.

gjcoram@nospam.mit.edu

✶ Risks of e-mail monitoring

Thomas Roessler <roessler@guug.de>

Wed, 8 Dec 1999 00:46:48 +0100

In some small firms, a simplistic approach may be applied to monitor employees' electronic mail: A responsible person inside the firm receives a copy of each incoming message, and possibly carbon copies of outgoing messages.

The privacy problems of this approach are obvious, however, they are not what this is about. In fact, there is another risk for the person who *receives* the message copies which is not completely obvious.

This risk is closely linked to the way in which most e-mail clients in

common use today display message overviews to users. In most cases, users are presented a list of message senders and subjects. The list of recipients is not shown, and no indication of the recipient is given, since the software assumes that every message in the user's inbox is intended for him. (There are exceptions from this, for instance the pine and mutt e-mail clients for Unix.)

Given no help from the software, the user will make up his own mapping from the information presented to him (i.e., subjects and message senders) to recipients. In particular, when there are some message senders who correspond with one or two employees on a regular basis, the person doing the monitoring will mis-recognize messages from these senders which are actually directed to her, and not to the senders' usual correspondence partners. The monitoring personnel may even delete these messages unread when the correspondence between the parties in question is not considered worth the effort of closer monitoring.

Given that the monitoring personnel might frequently be senior employees, this effect may even lead to the loss of particularly important e-mail messages sent by clients to these senior employees.

The cure? Use e-mail clients which tell you whether your e-mail is personal or not. Or, even better, use a reasonable e-mail monitoring policy which

- (1) avoids the privacy implications of the simplistic scheme and
- (2) makes

it possible to easily distinguish surveillance output from personal messages. Finally, senior employees may just be forced to read *all* messages which reach their e-mail inbox. However, this may not be an option depending on the amount of noise introduced by the monitoring.

⚡ Re: Counterfeit Japanese coins and resulting risk... (Opie, [R-20.67](#))

Henry Spencer <henry@spsystems.net>
Tue, 7 Dec 1999 18:59:14 -0500 (EST)

>The lesson to comp.risks? Of course, that assumption that a coin is a coin.

Unfortunately, merely returning the customer's own coin is not sufficient. Unless there are other restrictions, it's almost as easy for the crook to make some trivial purchase, requiring most of his supposed money to be returned as change. (This is a common counterfeiter tactic, although in the past it has usually been applied to humans rather than machines.)

Henry Spencer henry@spsystems.net (henry@zoo.toronto.edu)

⚡ Re: Ladbroke Grove ([RISKS-20.62](#))

Mark Brader <msb@vex.net>
Mon, 6 Dec 1999 17:37:44 -0500 (EST)

In the first item on the Ladbroke Grove rail accident, the number of deaths was given as "at least 70". It turned out that that number included a large number of people that simply *might* have been on the train and could not be immediately located. Based on information I got from Clive Feather, there were only 30 deaths that day (including the two drivers), plus one more who died from burns on 3 Nov 1999.

✶ USENIX Security Symposium 2000 - A Call for Papers

Moun Chau <moun@usenix.ORG>
Mon, 6 Dec 1999 19:39:27 GMT

9th USENIX Security Symposium 2000 Conference
August 14 - 17, 2000
Denver, Colorado, USA
Conference URL: <http://www.usenix.org/events/sec2000>

The USENIX Security Symposium brings together researchers, practitioners, system administrators, systems programmers, and others interested in the latest advances in security and applications of cryptography. The keynote speaker is Dr. Blaine Burnham, Director of the Georgia Tech Information Security Center (GTISC) and formerly Program Manager for the National Security Agency (NSA) at Ft. Meade, Maryland.

We are currently seeking submissions for Refereed Papers, Works-In-Progress Reports, Talks/Panel Session proposals, and Tutorial presentation proposals for this event. If you are working in any practical aspect of

security or applications of cryptography, the program committee urges you to submit a paper.

Please see the detailed author guidelines, which include a sample abstract, for more information.

<http://www.usenix.org/events/sec2000/cfp/guidelines.html>

* Paper submissions due: 10 Feb 2000

USENIX Security Symposium 2000 is sponsored by USENIX, the Advanced Computing Systems Association, in cooperation with the CERT Coordination Center. USENIX is an international membership society.

Call for Papers - Safecomp 2000

"Windt-Krose, Gemma" <g.j.m.vanderwindt-krose@tbm.tudelft.nl>

Thu, 2 Dec 1999 16:11:49 +0100

SAFECOMP 2000 Call for Papers

19th International Conference on
Computer Safety, Reliability and Security

October 25-27, 2000 ROTTERDAM, The Netherlands

Papers are invited on all aspects of state-of-the-art, experiences and new trends in the area of computer safety, reliability and security regarding critical applications of computer systems. Special topics include security relevant to safety, human factors, hardware solutions, verification & validation, distributed systems, and safety-critical y2k

experiences.

Special themes are on medical systems, transport & infrastructure systems, and software process improvement. Contributions from research, industrial applications and experiences, and on licensing questions are welcomed.

====> Paper submission DEADLINE: FEBRUARY 15, 2000 <====

MORE INFORMATION:

<http://www.wtm.tudelft.nl/vk/safecomp2000>

E-mail: safecomp2000@wtm.tudelft.nl



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 69

Thursday 16 December 1999

Contents

- [Biryukov and Shamir cryptanalysis of A5/1 GSM privacy algorithm](#)
[Matt Blaze](#)
- [Debit-card fraud in Canada](#)
[Steven M. Bellovin](#)
- [Croydon Tramlink: those signalling problems in full](#)
[Clive D.W. Feather](#)
- [Computer technology at the end of the 20th century](#)
[David Sedlock](#)
- [On the Internet nobody knows your five identities](#)
[NewsScan](#)
- [More CERT Advisories on buffer overflows](#)
[PGN](#)
- [Re: No bounds checking in Microsoft RTF controls](#)
[R A Downes](#)
[Mark Brader](#)
- [Macros in RTF files](#)
[Tom Hill](#)
- [Y2K-related viruses](#)
[PGN](#)
- [Power-out in Y2K test](#)

[Debora Weber-Wulff](#)

● [Risks of Y2K overreaction](#)

[Steven Huang](#)

● [Top 10 Risks search queries](#)

[Lindsay Marshall](#)

● [Go to jail - go directly to jail ...](#)

[Martyn Thomas](#)

● [According to Alta Vista, everything is for sale...](#)

[Daniel P. B. Smith](#)

● [Quicken's no-undo interface design](#)

[Timothy Prodin](#)

● [Risks of webbed e-mail and cookies](#)

[Lloyd Wood](#)

● [Windows98 censoring word processing apps](#)

[Eric Wagoner](#)

● [Re: Crack in GSM cell-phone encryption scheme](#)

[Boyd Roberts](#)

● [Re: DVD encryption](#)

[Brad Ackerman](#)

● [Re: Why computers are insecure](#)

[Durwin Sharp](#)

● [*Absent* source code now available](#)

[Avi Rubin](#)

● [CFP, 23rd National Information Systems Security Conference](#)

[Ed Borodkin](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ Biryukov and Shamir cryptanalysis of A5/1 GSM privacy algorithm

Matt Blaze <mab@research.att.com>

Thu, 09 Dec 1999 15:02:57 -0500

As RISKS readers probably already know, Alex Biryukov and Adi Shamir

announced that they have a practical cryptanalytic attack

against the A5/1 algorithm (which is the "strong" GSM privacy cipher). (Actually, the attack is against the version of A5/1 published at www.scard.org, which may differ from the version deployed in various actual GSM systems).

I've gotten permission from Adi Shamir to distribute a draft of the Biryukov/Shamir A5/1 attack paper, so it's now available (in PostScript format) on my web site:

<http://www.crypto.com/papers/others/a5.ps>

Assuming the Biryukov/Shamir attack against A5/1 works against the fielded version of the algorithm, routine, over-the-air monitoring of GSM traffic by even modestly-funded eavesdroppers should be considered a serious and realistic threat. This attack should represent another nail in the coffin for security systems designed in secret and not subjected to the scrutiny of the community. Had the A5/1 designers published their scheme in the open literature instead of trying to keep it secret, this weakness would likely have been discovered much sooner, perhaps before the cipher had actually been used to protect real traffic. One of the first lessons we teach cryptology students is that secret algorithms are a bad idea. Unfortunately, there are still people designing important systems who don't seem to grasp this basic principle.

Debit-card fraud in Canada

"Steven M. Bellovin" <smb@research.att.com>

Fri, 10 Dec 1999 22:12:27 -0500

According to the **Toronto Globe and Mail** (10 Dec 1999), a massive debit-card fraud operation has been detected in Canada. It involves doctored swipe readers that record and transmit the mag stripe information; they also record the PIN entered on the keypad. The operation is allegedly being run by organized crime.

The article noted that earlier schemes involved double-swiping (a recent news story in New York had someone arrested who used a suitably-modified PalmPilot for that), plus shoulder-surfing or concealed cameras to capture the PIN.

For details, see <http://www.globeandmail.com/gam/National/19991210/UDEBIN.html>

--Steve Bellovin

✶ Croydon Tramlink: those signalling problems in full

"Clive D.W. Feather" <clive@demon.net>

Mon, 13 Dec 1999 21:01:02 +0000

The opening of the new tram system in Croydon has been delayed due to a signalling problem. A poster on a UK newsgroup reports that the problem was a little unusual:

> When a tram was approaching traffic lights, the lights would automatically
> be set to red for other traffic flows: unfortunately, the

lights were not
> reverting to green after the tram had passed, so a single tram
passing
> once around the town centre would gridlock the roads for the
rest of the
> day.

Clive D.W. Feather, Demon Internet Ltd. Tel: +44 20 8371 1138

⚡ Computer technology at the end of the 20th century

"David Sedlock" <das@step.de>
Tue, 14 Dec 1999 14:14:27 +0100

I think this quote from Bill Bryson's "Notes from a Big Country"
pretty much
sums up computer technology at the end of the 20th century. I
believe that
Bill would allow us this "fair use" of his words.

"For a long time it puzzled me how something so expensive, so
leading
edge, could be so useless, and then it occurred to me that a
computer is a
stupid machine with the ability to do incredibly smart things,
while
computer programmers are smart people with the ability to do
incredibly
stupid things. They are, in short, a perfect match."

David Sedlock

⚡ On the Internet nobody knows your five identities

"NewsScan" <newsscan@newsscan.com>
Tue, 14 Dec 1999 08:43:55 -0700

Montreal software company Zero-Knowledge Systems (www.freedom.net) is now marketing software that will allow a person to use five different anonymous and untraceable identities on the Internet, preventing companies or agencies from using technology to track people's buying habits or other personal information. Of course, such software will also "make it a little more difficult to trace wrongdoers," as the National Association of Chiefs of Police makes clear. But privacy advocate Jason Catlett counters: "Anonymous speech is inconvenient and sometimes has bad consequences, but if you removed it we would be living in a very dangerous world." Zero-Knowledge says that spammers would not be aided by their technology, because a user of the software will be able to send only a small number of anonymous e-mail messages. [AP/*San Jose Mercury News*, 13 Dec 1999, <http://www.sjmercury.com/svtech/news/breaking/ap/docs/11846351.htm>; NewsScan Daily, 14 Dec 1999, reprinted with permission]

[Note that Canada's policies regarding crypto differ from those in U.S., so this product is generally freely exportable. PGN]

⚡ More CERT Advisories on buffer overflows

"Peter G. Neumann" <neumann@csl.sri.com>
Mon, 13 Dec 1999 15:59:13 -0800 (PST)

The spate of security problems related to buffer overflows seems to continue unabated. Two recent CERT Advisories may be of particular

interest to RISKS
readers.

CERT Advisory CA-99-15

Buffer Overflows in SSH Daemon and RSAREF2 Library

CERT Advisory CA-99.16

Buffer Overflow in Sun Solstice AdminSuite Daemon sadmind

CERT publications and other security information are available
from

<http://www.cert.org/>

Email: cert@cert.org

Phone: +1 412-268-7090 (24-hour hotline)

Fax: +1 412-268-6989

Postal address:

CERT Coordination Center

Software Engineering Institute

Carnegie Mellon University

Pittsburgh PA 15213-3890

U.S.A.

⚡ Re: No bounds checking in Microsoft RTF controls

R A Downes <main@radsoft.net>

Wed, 08 Dec 1999 19:24:45 +0000

A number of people have written and asked about the RTF utility,
when it
would be ready, if it ever would be ready, etc. Well now it is
ready, and it
can be downloaded at:

<http://32bit.bhs.com/download.asp?filename=Rtfboom5%2EZIP>

It's only about 10KB, so it should go rather fast. The program
acts as a
filter, but you have to "drop" your suspect files on it. All is
revealed

within the HTML documentation in the ZIP file.

RA Downes, Radsoft Laboratories <http://www.radsoft.net>

✂ Re: No bounds checking in Microsoft RTF controls (Meeroh, [Risks-20.68](#))

Mark Brader <msb@vex.net>

Wed, 15 Dec 1999 01:43:53 -0500 (EST)

```
>> ... I mean, this is very _basic_ programming, isn't it?
```

```
>>   for (cp = buf; cp < buf + BUFSIZE; cp++) ...
```

```
> [This] code fails in the subtle case when buf + BUFSIZE  
extends past the
```

```
> end of the address space. Note that the ANSI C guarantee that  
you should
```

```
> be able to compute the address of the first element beyond the  
end of a
```

```
> named array doesn't apply if buf is dynamically allocated. ...  
yet almost
```

```
> every programmer I've seen uses the same idiom for both cases.
```

```
> ... (See Writing Solid Code by Steve Maguire, p 132.)
```

And so they should, because this claim is simply wrong. The standard's

guarantee that `buf + BUFSIZE` provides a valid (though undereferenceable)

pointer "one past the last element" is independent of how the space is

allocated, and this has not changed as the standard has been updated.

The limitations on addition involving pointers are specified in section

3.3.6 of the original ANSI C standard, 6.3.6 of the first ISO version,

and 6.5.6 of the new standard; in all cases the wording refers to an

"array object". "Object" essentially just means a region of data storage (defined in section 1.6/3.14/3.14), and dynamically allocated space can certainly be accessed as an array (see section 4.10.3/7.10.3/7.20.3).

I suspect that Maguire misunderstood the standard's phrase "array object" and thought it meant what Meeroh calls a "named array".

Mark Brader, Toronto, msb@vex.net

✶ Macros in RTF files (re: Stewart, [RISKS-20.68](#))

Tom Hill <tomNOhillSPAM@worldware.com>

Wed, 15 Dec 1999 11:07:05 -0800

> >We'll pass CVs internally across to other "more sensitive" machines in .rtf
> >format (using rtf avoids Word-type macro viruses).

Be careful about your assumptions. If you save a Microsoft Word document as a .doc file, and then change the extension to .rtf, word will still open it, macros and all. Word is apparently smart enough to figure out the actual format of the file, and react accordingly.

The risk is that your users may assume that it is ok to open any attachment with an extension of ".rtf", since RTF files are 'safe'. Or your firewall may not filter out pseudo-rtf files for the same reason.

I'm using word 97, on Windows. I didn't test this with an auto-run macro, just verified that the macro warning message came up when I

opened the file
with the ".rtf" extension which contained the macro. (Note: You
might want
to turn on macro warnings from the tools menu/options/general/
macro virus
protection, if you haven't already.)

Tom

P.S. I did understand that apparently Ross was discussing the
case where
they do the conversion to RTF themselves, and so won't have this
problem,
but I still thought the risk worth noting.

[Lots of folks noted this one as well. PGN]

⚡ Y2K-related viruses

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

Wed, 8 Dec 1999 14:36:03 -0500 (EST)

Y2K seems to be a spawning ground for security attacks. W95.
Babylonia
is a virus masked as a Y2K fix. It has the ability to update
itself
remotely, and spreads through autodownloads in Microsoft chat-
room software
or e-mail. Other viruses posing as Y2K upgrades have also been
reported.
[Source: Self-updating virus spreads on Internet, AP item, 8 Dec
1999;
Courtesy of Sam Kasseman]

⚡ Power-out in Y2K test

Debora Weber-Wulff <weberwu@tfh-berlin.de>

Tue, 14 Dec 1999 13:07:36 +0100

The Berlin newspaper "tageszeitung" from Dec. 11, 1999 reports on a Y2K test conducted at the federal Department of Justice. The workers had been asked to not use their computers from 14.00 on Friday. Good thing, since the tests managed to shut down the power in the building. No one wants to make an official statement on the subject, since the official German policy is that "Everything is going to be all right".

<http://www.taz.de/tpl/1999/12/11/a0131.fr/text?re=ba> for those who read German "Millennium-Bug im Justizministerium"

Prof. Dr. Debora Weber-Wulff, Technische Fachhochschule Berlin
weberwu@tfh-berlin.de, <http://www.tfh-berlin.de/~weberwu/>

✶ Risks of Y2K overreaction

"Steven Huang" <sthuang@hns.com>

Wed, 8 Dec 1999 14:59:17 -0500

The human element of widely published risks like the Y2K problem has seen some coverage in RISKS, but seems to have been limited to predictions.

The *Philippine Daily Inquirer* and Associated Press report that a 61-year old retired government engineer, fearing the Y2K bug, withdrew his life savings of PHP2.8 million (about US\$69,000). Ten days later, four men slipped into his house and robbed him of his savings, plus some

PHP300,000

(about US\$7,400) worth of jewelry. This is a large amount of money in the Philippines, worth about a decent-sized new house outside the city.

First of all, it appears that the banking industry's assurances were insufficient to calm this educated man's fears. Secondly, even if you don't trust the banks, it's probably sufficient to convert the savings to cash (or better yet, cashier's check or manager's check) and put it away in a safe deposit box at your bank. Was information about the Y2K bug spread so poorly that an educated grown man was so scared he ignored a much more conventional Risk?

Steven Huang Hughes Network Systems, 11717 Exploration Lane, Germantown, MD 20876 MobileSat (240) 453-2357

Top 10 Risks search queries

<Lindsay.Marshall@newcastle.ac.uk>

Thu, 16 Dec 1999 14:12:40 +0000 (GMT)

- 10 hacking
- 9 ariane
- 8 virus
- 7 airbus
- 6 GPS
- 5 ATM
- 4 software failure
- 3 year 2000
- 2 Y2K
- 1 y2k

Aren't we all so predictable!

<http://catless.ncl.ac.uk/Lindsay>

⚡ Go to jail - go directly to jail ...

"Martyn Thomas" <mct@hollylaw.demon.co.uk>

Sun, 12 Dec 1999 23:41:25 -0000

A recent Spam e-mail called "free world site" gave me a shock. In Outlook 98, simply selecting the message (to delete it) executed the HTML it contained, which used the OpenWindow function to connect to a remote Web site.

The risk? In the UK, according to the BBC radio news, several people have recently been arrested "in co-ordinated raids across the country" for downloading child pornography from the Internet. They were apparently found by monitoring Net traffic, and part of the evidence against them is the record of web-sites visited "automatically stored on their computer's hard disk".

Then again, there's all the other things you can do with HTML.

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

⚡ According to Alta Vista, everything is for sale...

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

Mon, 13 Dec 1999 21:00:34 -0500

I did an Alta Vista search on the phrase "priesthood of all believers"

and was somewhat surprised when Alta Vista invited me to:

"Comparison Shop! - Find products and compare prices for 'Priesthood of all believers'"

I tried "members of Congress" and, sure enough...

"Comparison Shop! - Find products and compare prices for members of Congress"

A search on "Love," as expected, invited me to

"Comparison Shop! - Find products and compare prices for love"

but it also said:

AltaVista knows the answers to these questions:
Am I in love?

"Daniel P. B. Smith" <dpbsmith@bellatlantic.net>
Lifetime address dpbsmith@mit.alum.edu

⚡ Quicken's no-undo interface design (Re: Welsh, [RISKS-20.67](#))

"Prodin, Timothy (T.R.)" <tprodin@ford.com>

Tue, 7 Dec 1999 16:55:43 -0500

> It does not even have the "Undo" feature which, starting in word
> processors and text editors, has come to be expected in all
> well-written
> Windows applications.

As it shouldn't. Consider that Quicken has designed their

register to
behave exactly like a real pen and ink ledger.

When entries are made in an old-fashioned ledger; they are immediately committed, by the virtue of writing the the registry entry. If a mistake is made, you must void the transaction - you can't undo it.

In this case, Quicken has done the right thing. A bank ledger is not a word processing document; and therefore it should not have the same interactions that word processors have.

[We received a slew of messages on this topic, plus a few snide remarks on the oxymoronicism of "well-written Windows applications". PGN]

⚡ Risks of webbed e-mail and cookies

Lloyd Wood <eep1lw@surrey.ac.uk>
Thu, 9 Dec 1999 00:55:25 +0000 (GMT)

A while back, I received a couple of free e-mail accounts on ZDNet Mail, which has previously been mentioned in RISKS [McGlothlen, R-19.74].

A while after that, ZDNet Mail become ZDNetOnebox, with a completely new database system and a new interface, requiring javascript enabled to do something as get help to find out why something as simple as deleting mail doesn't work (because you haven't got javascript on, of course - a risk in itself). I now have some US phone, fax and voicemail facility I'll never use

either too.

Both accounts were migrated to this new interface. A redirect from www.zdnetmail.com to www.zdnetonebox.com was implemented, but I'd never gotten around to updating my bookmarks.

ZDNet Onebox uses session management with cookies. Imagine my surprise, after accessing one account, selecting the menu entry corresponding to www.zdnetmail.com from my browser's bookmarks menu, and logging in with name and password for the second account, on being presented with the contents of the mailbox of the `_first_` account.

Risks lie in assuming that only one person uses a browser session, that that person will be able to sign off to force the end of the session, and that session information is more important than any user-supplied information that overrides and cancels it.

(If I update my bookmarks, I'll see the mailbox contents immediately, without the chance to login. some risks of assumption and complexity here.)

The other associated risk with ZDNet Onebox is the constant stream of Jesse Berst e-mails that I'd swear blind I never signed up for.

... but hey, at least it's not Hotmail, right?

<L.Wood@surrey.ac.uk>PGP<<http://www.ee.surrey.ac.uk/Personal/L.Wood/>>

Windows98 censoring word processing apps

"EricWagoner" <ewagoner@partnersoft.com>

Wed, 8 Dec 1999 11:40:36 -0500

A friend of mine recently bought a new Gateway computer for his family. He's a playwright and an English professor, and so does plenty of writing. The computer came pre-installed with Microsoft Word 97, which he was beginning to get comfortable with. He told me the other day that he was having a problem he needed help with -- he was writing a script that contained a character with a mild potty mouth, but every time he wrote the "S-word", it got instantly replaced with XXXX. What's worse, in another script, a period piece with archaic English, MS Word would replace those four letters with XXXX even if they were parts of two different words, such as "'Tis hit!". These four letters show up surprisingly often in English of a few hundred years ago, and this was driving him crazy.

I thought it was a simple matter of setting the auto-correct feature in MS Word, that maybe cuss words were now censored by default. I told him how to disable the feature, or at least how to remove those letter combinations from the lists. He told me a few days later that it didn't help, that even with auto-correct completely shut off he was still plagued with XXXXs in his scripts. I told him I'd gladly come over and take a look.

When I did, I found he was correct, that I had told him wrong. I scoured Word for some kind of "child protection" feature, but could find

nothing

anywhere. Out of curiosity more than anything, I opened WordPad and tried to type the word, and it was instantly replaced with XXXX. I opened NotePad, and again XXXX. I realized then that it was a global Windows 98 setting and had nothing at all to do with Word. In the control panel, I looked in Users, Accessibility Options, and anywhere else I could think to look for child protection features, and came up blank. Finally, I noticed that in the Start menu was the item "Log Off DEFAULT". It struck me that in all the many times he and his family had booted up the computer since he bought it, no one had logged into Windows under their own name, that everyone was using the DEFAULT user.

I restarted Windows and logged in as "eric". All of the XXXXing was gone, and I was free to type what I wished. I logged on again as DEFAULT, and censoring began anew. I gave him the solution, and he was happy.

I've now scoured the web for some mention of this "feature" but have found nothing. I tried logging on as DEFAULT on my own computer, and when Windows started I got an error (advpack not started -- missing dll -- something like that), so it seems that this may be something built in by Microsoft for some reason. The only thing I can guess is maybe it's for store floor models so some kid can't go leaving dirty graffiti on the screens. Of course, Gateway sells direct by mail-order, so that's not an issue here.

Anyone ever heard of this before? Certainly, real professional work was

being prevented by this seemingly undocumented feature. Interestingly, very few words were censored in this way. I could be plenty raunchy with nary an interference, but say the "S-word" or what CAP calls the "most foul of foul" words, and I was silenced.

Eric Wagoner <ewagoner@partnersoft.com> <http://www.partnersoft.com>

Partner Software; Kestrel's Nest Weblog <http://www.athens.net/~ewagoner>

[And all that XXXXing is likely to get THIS issue censored! PGN]

⚡ Re: Crack in GSM cell-phone encryption scheme

<boyd.roberts@ca-indosuez.com>
Thu, 9 Dec 1999 13:00:39 +0100

an Omnipoint executive says, "What they're describing is an academic exercise that would never work in the real world. What's more, it doesn't take into account the fact that GSM. calls shift frequency continually, so even if they broke into a call, a second later it would shift to another frequency, and they'd lose it."

Yes, there is frequency hopping, but it is slow -- and that it is not significant with respect to the modulation (i.e., the 600us bursts every 1.2ms). The 'executive' admits just that; 1 second is insignificant when compared to the 600us bursts.

The frequency hopping may not be turned on.

The hopping sequence can be learned over the radio link from the BTS. I

forget if this is in the clear or encrypted with A5 during an exchange with

the BTS. I don't think it really matters whether it's in the clear on the

BCCH or encrypted with A5; once A5 is cracked all bets are off, provided you

can do it in real time. It appears they can.

I've had this discussion before with people that you can't build a GSM

scanner. Each time I've picked up my mobile and said 'What's this?

It's a GSM scanner'. It has a few clues about where to look, but now

it would appear that everybody can get them.

Boyd Roberts

boyd.roberts@ca-indosuez.com

✦ Re: DVD encryption (Graifer, [RISKS-20.67](#))

Brad Ackerman <bsa3@cornell.edu>

11 Dec 1999 23:13:44 -0500

> ... They have failed at this by opting for security by
> obscurity and not

> employing the publicly reviewed techniques.

This isn't quite the issue. No matter what protocols or algorithms are

used, fully working copy protection (barring armed guards stationed at the

playback device) is impossible. Every DVD player must be able to decrypt

and play the DVD with no additional information, which means that no matter

how strong the actual encryption is, the key must always be available to anyone who cares to look. Unless the decryption is implemented in tamper-proof hardware, the resources required for key extraction are well within the range of "casual pirate[s]." Of course, since such hardware is not known to exist, and would be far too expensive for consumer devices if it did, the studios will just have to live with easily copyable media, as the software industry has been doing for some time.

Brad Ackerman N1MNB bsa3@cornell.edu

✉ Re: Why computers are insecure (Schneier, [RISKS-20.67](#))

<durwin@exxon.com>

Thu, 9 Dec 1999 07:54:51 -0600

Much worse, it applies to physical sciences as well. I first ran across this idea many years ago reading Karl Popper, *The Logic of Scientific Discovery*. His basic premises are:

- Physical "laws" are actually hypotheses stated in a manner that allows independent testing of specific physical (observable) phenomena.
- No matter how often a hypothesis is tested, it can never be proven. It only takes one contrary observation to invalidate a hypothesis that had previously been accepted. A useful anecdote relates to the amount of "proof" provided for Newtonian physics over many years -- until Einstein

said, "wait a minute, this doesn't work and I have a different hypothesis".

In order to conduct our daily lives, we have to accept many hypotheses that have been corroborated, but not proven -- as Newtonian physics, they are good enough for our normal use. As our knowledge and understanding grows, some "laws" may fall to new understanding (read: hacks) while others survive to fall another day. The set of hypotheses we choose to accept as "laws" is determined by the level of risk we are willing to assume, in the world and in security.

DURWIN SHARP, Exxon Mobil Corporation, P. O. Box 4276,
Houston, TX 77210-4276 USA 1-713.656.6969 durwin@exxon.com

***Absent* source code now available**

Avi Rubin <rubin@research.att.com>

Fri, 10 Dec 1999 00:35:57 GMT

We are pleased to announce the public release of the Absent, secure remote access system. A description, the paper, and the code are available at

<http://www.research.att.com/projects/absent>

Absent is a system for secure remote access to the internal web from outside. It addresses the problem of secure remote access to a site's internal web server from outside the firewall. The goal is to give authorized users access to sensitive information, while

protecting the information from others. We implemented our solution using a one-time password scheme for client authentication and SSL for confidentiality. Our main design considerations were security, performance, ease of use, availability, and scale. We were further constrained by the desire to leave our firewall and local infrastructure unchanged.

Christian Gilmore, Dave Kormann, Avi Rubin
AT&T Labs - Research

✶ CFP, 23rd National Information Systems Security Conference

"Ed Borodkin" <borodkin@constitution.ncsc.mil>
Tue, 14 Dec 1999 14:55:26 -0500

CALL FOR PAPERS, PANELS, TUTORIALS, AND WORKSHOPS

Co-sponsored by the National Computer Security Center and National Institute of Standards and Technology

Week of 16-20 Oct 2000, Baltimore Convention Center, Baltimore, MD

The National Information Systems Security Conference welcomes papers, panels, tutorials, and workshops on all topics related to information systems security. Our audience represents a broad range of information security interests spanning government, industry, commercial, and academic communities.

See <http://csrc.nist.gov/nissc/call.htm> for instructions on sending your

submissions.

Ed Borodkin, Program Director, NISS Conference <http://csrc.nist.gov/nissc/>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 70

Sunday 19 December 1999

Contents

- [ResearchIndex: a digital library of computer science papers](#)
[Ursula Martin](#)
- [Where do you want to go today ? And... when exactly ?](#)
[Nick Brown](#)
- [Another appalling Web security story](#)
[Nick Brown](#)
- [Risks of US-Euro date conversion](#)
[Terje Mathisen](#)
- [Re: Melissa perpetrator faces five years in prison](#)
[Russ Cooper](#)
- [Y2K fear vs. Common sense](#)
[identity withheld](#)
- [Browsers should only display what is requested?](#)
[Dick Shelton](#)
- [Netscape and the risk of two accounts](#)
[Steven J. Greenwald](#)
- [RST discovers defective crypto in Netscape mail](#)
[Zygo Blaxell](#)
[Raymond Michiels](#)
[Michael Kohne](#)
[Gary McGraw](#)

[John Viega](#)

[Dan Foster](#)

• [Info on RISKS \(comp.risks\)](#)

✶ ResearchIndex: a digital library of computer science papers

Ursula Martin <ursula@csl.sri.com>

Thu, 16 Dec 1999 12:01:02 -0800

ResearchIndex <http://citeseer.nj.nec.com/cs> is a digital library that harvests documents from web pages (220,000 so far), builds a citation index (over 2.5 million so far) and provides text search. Each document has a page which gets you the original URL, a cached copy of the document, backwards citations, forward citations in context and links to other documents that are related or have substantial matching text.

On the one hand this is a fascinating, audacious and extremely useful resource. On the other such digital libraries and research tools (and this research prototype in particular), and the radical new model of accreditation, access, and authentication for scientific information that they can potentially support, raise significant and far reaching security, rights and privacy questions for the scholarly community.

For example look again at some features of ResearchIndex :

* Anyone, apparently without authentication, can add so-called "Authors" comments and "Title correction" to any document record or suggest new URLs for ResearchIndex to harvest. Digital libraries need robust security and authentication mechanisms if they are to be a

trusted part of the scientific process.

* A "most cited" list: pause a moment, before awarding "J Smith" tenure on the basis of that spectacular Number 16 position, which is the result of concatenating several different people, to reflect on the problems of name reconciliation and the dangers of relying on unauthenticated data, particularly in matters that may be subject to legal challenge.

* It provides a listing of what "Users who viewed this document also viewed": so think twice before using ResearchIndex to investigate that potential patent involving a novel application of YYY to the entirely unrelated ZZZ. Wonder about the "right of a scholar to the privacy of the study", and recall the privacy conventions about access to library borrowing records in your own state or country. Consider what such a service could or should track and analyse, what use might be made of such tracking information and who has rights to it: for example what if analysing usage patterns made a connection that beat someone else to a patent?

* It caches copies of the documents, which are then available for download. Question exactly what versions of which documents have been harvested from where, and how accurate the analysis is: ResearchIndex gives one of my papers a bizarre ``Abstract'' consisting of the paragraph following an occurrence of the word ``Abstraction''. Wonder what happens when a document is later removed from the URL it was harvested from, for example for copyright reasons. Then figure out the authentication and rights issues.

* Think about what is not there: for example citations of Turing's papers (he is Number 4101 in the most cited list), but not the papers themselves, and reflect on the future of our paper archives and libraries.

We expect our on-line documents to be located, read and analysed by people and machines, that is why we put them on-line. Sooner or later there will be a production version of something like ResearchIndex that addresses these problems, but meanwhile we all have a chance to debate what we want, and the authentication, security, rights, privacy, legal and political implications of the "harvesting", mining and distribution of the world's on-line research documents.

Starting points for further reading:

The Coalition for Network Information has many relevant reports at

<http://www.cni.org/projects/>

Henry Gladney, Safeguarding Digital Library Contents and Users, Interim Retrospect and Prospects, D-Lib Magazine, July/August 1998

<http://www.dlib.org/dlib/july98/gladney/07gladney.html>

Ursula Martin University of St Andrews/SRI

⚡ Where do you want to go today ? And... when exactly ?

BROWN Nick <Nick.BROWN@coe.int>

Fri, 19 Nov 1999 10:19:19 +0100

Microsoft Outlook has a feature which allows you to tell the

Exchange server

to deliver a mail after a certain time. For example, you could use this to send your company's quarterly results to the press at 7am tomorrow and be sure they would not go out until the figures are officially published.

However, due to a problem in the definition of time (!), it is possible for the delivery time to be an hour late or an hour early. An hour late is perhaps not so bad - after all, you said "do not deliver before 7am", and it's true, 8am is not before 7am. But an hour early? Can you say arbitrage?

The problem is that all events in Exchange are scheduled in GMT, but Exchange does not correctly handle the automatic changes in the Windows NT system clock when daylight savings time kicks in. The result is that, after daylight savings time starts or ends, and until you reboot your Exchange server:

- deferred mails sent in the fall, when the clocks go back, will be delivered an hour later than you expected.
- deferred mails sent in the spring, when the clocks go forward, will be delivered an hour earlier than you expected.

The workaround is, of course, to reboot your Exchange server (or completely restart Exchange, which involves more or less the same level of user downtime) when the time changes. But on sites which have a policy to reboot only one major server at a time (there are several good reasons

to do this),
this could take several days (Exchange servers are notoriously
slow to
shutdown).

Doubtless Microsoft's preferred permanent fix is to lobby
governments to
abolish daylight savings time. Hmmm... isn't the French
government pretty
keen on that right now ? Is that what Bill was talking to
Chirac about ?

Nick Brown, Strasbourg, France.

for more information, <http://dct.coe.int/info/emfci001.htm>

✶ Another appalling Web security story

BROWN Nick <Nick.BROWN@coe.int>

Fri, 10 Dec 1999 10:49:36 +0100

The home exchange organisation to which I belong has decided to
put its
catalog online. Anyone will be able to view the homes which are
offered,
but contact address and phone number details will be provided
for members
only.

Today I received the instructions for logging on. Hoo boy -
here we go
again:

- The Username is your country code followed by your membership
number
within the country. This is published in the paper catalogue.

- The Password is "xxxxxxxx" (I have censored it). But - the
password is
the SAME for EVERY username. You read that correctly.

So, the usual list of RISKS:

1) Member US1234 can log on as Member US5678. In theory this is no big deal because currently all you can do is read information which you could have obtained as the other member, although for auditing reasons I'm sure they'd like to know who is really logging on. But we are promised that in future versions, we will be able to update our site entries ourselves...

2) Non-member Z can very easily obtain a member number. And even if the site managers notice that Member US1234's account is being used by 500 PCs a day after someone posted it to DejaNews, and they close that account, it will not require a degree in computer science to work out that US1235 etc are worth a try, since there's none of the usual hassle to guess the password.

Needless to say, I have asked the organisation to remove me from the Web site immediately.

Nick Brown, Strasbourg, France.

for more information, <http://dct.coe.int/info/emfci001.htm>

⚡ Risks of US-Euro date conversion (Re: Ben Hines, [Risks Digest 20.67](#))

Terje Mathisen <Terje.Mathisen@hda.hydro.com>

Wed, 08 Dec 1999 12:48:21 +0100

This is really just another of the risks we face from not

adopting
proper standards (i.e., satellite failure caused by US/Metric
conversion error)

In the case of dates, we have had an international (ISO)
standard for many
years now, according to this dates should be displayed as 1999-
12-10 instead
of 12/10/99 or 10/12/99 or even (heaven forbid!) 01/02/03.

Here's one page showing some of the problems related to our
current mess,
and why all countries, not just Japan and Sweden, should switch
to ISO
8601. This page also have links to the full standard text.

<http://www.saggara.demon.co.uk/datefmt.htm>

Terje

PS. The corporation I work for, Hydro, very sensibly decided
some years
ago to switch to ISO dates, even though this is different from
the
Norwegian standard.

<Terje.Mathisen@hda.hydro.com>

Using self-discipline, see <http://www.eiffel.com/discipline>

⚡ Re: Melissa perpetrator faces five years in prison ([RISKS-20.68](#))

Russ <Russ.Cooper@rc.on.ca>

Wed, 15 Dec 1999 09:27:09 -0500

IMO, there many risks that the case against Mr. Smith for
Melissa may
bring to reality.

1. That a GUID may be accepted in court as a "signature" uniquely

identifying a particular human being. At best the GUID is circumstantial, and it is far too easy to show GUIDs belonging to others (mistakenly or intentionally) resident on your machine.

2. That it may be accepted as possible to prove the route which a particular virus has traveled to get to the point where it is deemed "in the wild", and presumably therefore actionable, solely on the basis of computer evidence.

2a. What is the crime? Making the virus, or releasing it "in the wild"? Surely making a virus is not a crime, so the test comes down to proving who released it "in the wild". Since that action must be done with intent, computer data alone, demonstrating that a particular file originated from a particular disk, still does not prove intent. If I were to co-opt Peter's machine and use it to send a virus to a Usenet list, should Peter be held liable for the damages of the virus?

2b. How is it proven? Computer data is malleable, and while Word documents may store revision information, and even information from RAM totally unrelated to the original document, it is possible that all of that information can be placed into another file either in addition to, or replacing, the 2nd document's original information. As such, it is again circumstantial evidence of origin and even ownership.

It is quite easy to villainize virus writers and infectors in the same way "two Arab men" were responsible for the Oklahoma bombing. An entire industry

is available for testimony as to the damage suffered by Corporate America every day as a result of the actions of the few virus writers. The NIPC, and therefore the FBI, are desperate to show they have the savvy to catch Cyber-criminals and justify their stance and actions.

IOWs, there's a significant weight against Mr. Smith if we allow prosecution testimony to go unchallenged for the vapor-thoughts it may well be. It must be shown that such conclusions, based solely on computer data, can easily be manufactured against anyone.

I have thought long and hard about how it may be possible to prove an individual is guilty of a particular computer crime. A confession, today, could be given simply to garner the publicity and reap the benefits after the jail term is served (do you think any conference would not pay to have Mr. Smith talk after he was released, if he could speak intelligibly? ... book deals ... guest spots ...) Criminals used to take the rap and not talk in order to get the loot when they were released ...;-]

Without another human being present during each of the steps required to release a virus into the wild with malicious or harmful intent, a conviction on circumstantial computer evidence would lead to many serious problems, IMO.

If the above evidence, assuming its present and the basis of the case against Mr. Smith, is accepted in court and the jury finds its credible, it will be far too easy to convict innocent individuals of computer

crimes in
the future.

Smith may well be guilty, and he is not my focus here. We must ensure that his conviction does not establish the wrong precedence's, lest we give the "enemy" the ammunition to get each and every one of us convicted of something, somewhere, based on the same quality of evidence.

I remind you that I, like most of you, have not seen the evidence against Mr. Smith and this is based solely on the media reports about its content ... therefore, I may be totally off-base ... but the risk is real no matter.

Russ - NTBugtraq Editor

⚡ Y2K fear vs. Common sense

identity withheld <>

Fri, 17 Dec 1999

I work for a large health maintenance organization. We share our campus with about a dozen other assorted companies. All of our upper management is absolutely terrified of the end of this year. They are convinced that there is going to be a major disaster at the stroke of midnight.

To deal with a potential loss of power, we have installed a generator onsite. A storage tank next to the generator holds 1,500 gallons of fuel. An additional 2,000 gallons of fuel will be parked next to the generator the entire weekend of the new year.

The risks?

1) The generator is in a hastily built wooden hut secured with a padlock.

The hut is located on the outside wall of our data center.

3,500 gallons of

boom.

2) One of the other clients on a campus constantly gets bomb threats.

Often the threats are real. Who needs a Rider Truck?

3) Disaster recovery planning has taken a back seat to Y2k planning. We

would not survive the loss of our data center. The disaster plans have not

been updated to reflect our move from VMS to Unix over the last 5 years.

4) People ignore the large "No Smoking" signs posted on the generator

shed. See #1. Who needs terrorists?

The Unix team has started parking on the far side of the parking lot

in the 'blast shadow' of another building.

[⚡ Browsers should only display what is requested? \(Re: Galt, RISKS-20.66\)](#)

Dick Shelton <dicks@shavliktechnologies.com>

Mon, 13 Dec 1999 16:22:19 -0600

"No browser has any business ever loading a URL unless the user requests it!"

That sounds non-controversial -- but what constitutes a request?

- o Typing it in the navigation window? Surely.

- o Clicking on a hyperlink? Probably (else hypertext becomes rather lame)
-- but what if the user doesn't recognize it as a link? And how many users routinely screen the reference before clicking the link? Typically there is not enough information available to know just what a link will get you into.

- o Automatically loading images for embedded tags? Well, there are times you wish it wouldn't, given the image bloat on the net, but the alternative is not very attractive either.

- o What about loading a URL in response to an onclick event? Or loading a new image in response to a mouseover event? As these are embedded in script or applets or components, it would be hard for the browser to distinguish between "requests" from the program and requests from user interaction. The alternative seems to be restricting user interaction to clicking on anchor tags. This is akin to restricting computer interaction to TTY mode. Sorry, but we've passed that stage.

In the current state of the net there is no incontrovertible notion of what constitutes a request. There will always be a natural tension between the convenience (and power) of the user interface and the problems of letting a program decide how to proceed. You can push the extremes too far in either direction.

Dick Shelton, Shavlik Technologies dicks@shavlik.com

✶ Netscape and the risk of two accounts

"Steven J. Greenwald" <sjg6@gate.net>

Sat, 18 Dec 1999 00:16:37 -0500

I use Netscape running on a Win95 platform to read most of my mail from a particular account with a particular ISP.

Recently I needed to get a second account from that same ISP (for a civil-rights group I'm working with).

I set up another Dial-up Networking connection using Win95, with this new user name and new password.

To test it, I connected to the new account. Everything seemed fine. I then clicked on the "Get Mail" icon in Netscape Messenger to get any mail that might be in the new account (typically there is a welcome message from the ISP).

Imagine my surprise when what came in was all the mail from my first account!

Of course, it turns out that Netscape stored (without my knowledge) the password to my first account internally (as has been noted previously in RISKS - I've just gotten around to reading that digest). Okay, I can understand that (but not agree with it).

But why did it use the first user name and password when the Win95 dial-up networking program connected to a completely different account

(I called my
ISP, and I was indeed connected to the new account)?

The risks are obvious. In any event, users should be told that their passwords are being stored by application code and that mail can be retrieved from one account via another without doing anything so esoteric as using telnet.

There just no accounting for this.

--Steve Greenwald <http://www.gate.net/~sjg6>

✶ RST discovers defective crypto in Netscape mail (McGraw, R-20.68)

Zygo Blaxell <uryse0d5@umail.furryterror.org>
Wed, 15 Dec 1999 05:56:47 GMT

> Unfortunately, the encryption algorithm used by Netscape to
scramble
> passwords is exceptionally weak.

Even if it weren't weak, it would still be equivalent to a plain text password. Netscape has to be able to send the password in the clear over the IMAP/POP3 protocols, so no matter what encryption mechanism is used, Netscape can always be reverse-engineered to retrieve the encryption algorithm and/or keys required to extract the password.

✶ Re: RST discovers defective crypto in Netscape mail password

saver

Raymond Michiels <raymond@frontier.nl>

Thu, 16 Dec 1999 21:42:38 +0100 (MET)

In defence of Netscape, I would like to point out that the only viable alternative to Netscape's "exceptionally weak" encryption is "security through obscurity." Storing passwords locally is inherently insecure.

Once again, those UNIX people have solved this one in a particularly elegant way using the ".netrc" file: store unencrypted passwords in a file which may only be readable to the owner. The level of security is immediately obvious to the user; the user can then make an informed decision to live with this security or to type the password whenever needed.

✶ RST discovers defective crypto in Netscape mail (McGraw, R-20.68)

Michael Kohne <mhkohne@discordia.org>

Thu, 16 Dec 1999 07:46:05 -0500

Not to seem silly but: So what? I'm no crypto expert, but it seems obvious to me that if the password is being stored on your machine and requires no other input from you for Netscape to provide the password to the other end, then it's by definition insecure.

No matter what crypto algorithm Netscape uses, ALL the secrets are on your machine - the encrypted password AND the code and secrets needed

to decode
it. Yes, it would take more time to reverse engineer the
relevant portions
of Netscape code than to simply break the algorithm the way you
did, but
only one person has to do so - then security is blown just the
same.

It doesn't matter that Netscape's local password storage isn't
secure - ANY
local password storage is going to be insecure. No matter how
complicated
the lock, if you hang the keys (or a technical manual on the
lock's
operation) on a hook next to the door, it doesn't do you much
good. The only
thing that encryption of the stored password prevents is
accidental
revelation during registry browsing.

And yes, the only workaround is to not allow Netscape to
remember your
passwords. But that's what you need to do. In all programs.
Always.

It should also be noted that if I'm not mistaken, the POP
protocol (I don't
know about IMAP) transmits the password in clear text. So all
someone needs
is a sniffer somewhere in between you and your mail server (like
your local
lan) and the results are the same.

It is a good thing to have folks like you point out security
holes in well
known applications, but I'd have to say that Netscape isn't as
terrible as
you make out on this one. All they did is decide that protecting
the
password in the local cache wasn't worth a lot of effort. And I
have to
agree with that sentiment.

On the flip side, Chris Saito's statement about recovery was just silly, as you rightfully point out.

One other point: In Risks you mention a Javascript based attack. Are you referring to using one of the known Javascript attacks to capture the user's encrypted password entries, or do you have something new?

Michael Kohne <mhkohne@discordia.org>

✂ RST discovers defective crypto in Netscape mail (McGraw, R-20.68)

Gary McGraw <gem@rstcorp.com>

Thu, 16 Dec 1999 09:30:15 -0500

You are correct Michael, there is NO perfect solution here. However, we believe using a well known crypto algorithm like DES and hiding the key material throughout the code is orders of magnitude better than Netscape's current approach. In other words, you raise the bar significantly by forcing people to reverse engineer for an attack (to find the key) and get much lower risk that way. The current approach is just too risky.

Along those lines, Avi Rubin (ATT Research) said it best when he said Netscape needs to run out and get a bar so they can raise it! We agree. Of course the "one attacker is all it takes" comment you made remains completely accurate.

With regards to the Javascript attack, we were referring to an

old
(presumably fixed) Javascript attack which was able to snag the
"encrypted"
password and lots of other private information from the prefs
file. Because
of Netscape's "patch through release" approach, the attack still
works
against Netscape 4.0 through 4.04. Yet another reason to update
your
browser.

Yesterday we were informed that Dave Edis of Interactivetools
created a
Web-based password cracker (which requires someone to enter the
obscured
password through a dialog box) at least a year ago. We were not
previously
aware of his work. Though his code does not work against
current versions
of Netscape, the algorithm currently used (and cracked by us) is
very
similar. See: <<http://www.thewebmasters.net/mailpass.html>> One
might wonder
whether this implies that Netscape is taking an arms race
approach to
obscuring the POP3 password. If so, why the heck not use DES??

As for sniffers, I believe you are correct about POP3 and
plaintext
passwords. Yet another serious risk, but compounding not
mitigating the one
we raised. Ain't shrinkwrap wonderful?

Gary McGraw, Ph.D, Vice President, Reliable Software
Technologies, Dulles, VA
gem@rstcorp.com <<http://www.rstcorp.com/~gem>> <<http://www.securingjava.com>>

🔥 RST discovers defective crypto in Netscape mail (McGraw, R-

20.68)

John Viega <John@list.org>

Thu, 16 Dec 1999 09:20:03 -0800

Let's be honest, the only thing you need to do to exploit this bug even without a JavaScript flaw in the person's browser is to trick the user into running some code on his machine. That's not too tough. I can e-mail all my friends a "dancing pigs" demo, and 90% of them will run it. That's a given.

Of course, if you can run code on other people's machine, there are lots of things you can do. The reason why this bug is a bigger problem is that POP/IMAP account info often doubles as a unix account. Also, people reuse their passwords on multiple accounts. Basically, this bug makes it much easier for a hacker to spread to new machines once one machine has been compromised.

> Yesterday we were informed that Dave Edis of Interactivetools created ...

I think that current WINDOWS versions might be more accurate. We only broke Windows encryption. Unix and Mac versions were slightly different; Windows pre-4.0 or so was different as well. We could tell it was similar, but not quite as complex. The primary difference seemed to be that there was no permutation of the bits.

When we talked to Netscape, we were told they knew the algorithm could be a lot better, but they were hoping it was unlikely anyone would target it and break it. They never indicated that they knew about their old cipher being broken, either, but I'd bet they knew

about it,
prompting the changes that led to the current algorithm.

> As for sniffers, I believe you are correct about POP3 and
plaintext ...

I didn't catch the original message, so I hope my response is
appropriate.
Sniffers are a big problem, but they generally require a person
to have
compromised administrative access on one machine on the local
network to
exploit. It can also be hard to mine the data, and there are
reasonable
detection techniques for sniffers (see l0pht's antisniff). In
short, I
think it'd be a fair bit easier for script kiddies to take
advantage of this
problem (assuming someone has given them a nice compact exploit)
than to
break in, install a sniffer, and retrieve and mine the results.

⚡ Re: RST discovers defective crypto in Netscape mail password saver

Dan Foster <dsf@gblix.net>

Wed, 15 Dec 1999 02:57:21 -0500

That's an excellent advisory regarding seemingly securely
encrypted passwords
by Netscape Communicator. Unfortunately, that particular issue
was already
previously discovered by others, as evidenced by BUGTRAQ
mailings around
November 7th and 8th, 1998 by Holger van Lengerich <gimli@uni-
paderborn.de>
and Thievco <thievco@sprite.netnation.com>. Credit where it's
due and all.
I seem to recall having also seen a C source file via BUGTRAQ

before to
decode the stored password, too.

Also, the referenced link at <http://www.rstcorp.com/news/bad-crypto.html>
returns a 404 Not Found error.

I'm not sure that saving passwords is a bad thing per se; it is possible to approach this through technological means, but seems it would be better addressed by policy means such as user education and policies on diversity of passwords for various accounts, as well as better suggestions for (user) memorable passwords. Or in the very least, put up an initial one time dialog box strongly discouraging the use of the option.

That said, XOR'ing the password does seem somewhat weak, and the RISKS of employing either poor choices for passwords or storing them in a less than secure manner without making noise about it to users seems obvious.

Dan Foster <dsf@gblix.net>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 71

Friday 31 December 1999

Contents

- [First real Y2K clock problem...](#)
[Peter da Silva](#)
- [Whoops! Auckland Awkward Awk!](#)
[John Wharton via Dave Farber](#)
- [Game Over at end of millennium...](#)
[John Elsbury via Dave Farber](#)
- [Credit-card machines in U.K. confused by Y2K](#)
[NewsScan](#)
- [Y2K claims early victims](#)
[John Locke-Wheaton via Dave Farber](#)
- [Pentagon Y2K preparations](#)
[Dave Stringer-Calvert](#)
- [Oakland CA 911](#)
[John Wharton via Dave Farber](#)
- [Two possibly unaddressed Y2K problems](#)
[Brett Glass via Dave Farber](#)
- [Low-tech Y2K failure](#)
[Earl Truss](#)
- [Risks of expiring digital certificates in older Web browsers](#)
[David Tarabar](#)

- [Shirley you can't mean this date is bad!](#)
[Conrad Heiney](#)
 - [The risks of last minute Y2K patches](#)
[Matt Blaze](#)
 - [Re: Y2K fear vs. Common sense](#)
[Scott Nicol](#)
[Eric Roesinger](#)
 - [Abolishing leap-seconds](#)
[Rob Seaman](#)
 - [Is the connection secure or isn't it?](#)
[Don Byrd](#)
 - [Privacy broken by Sanity.com](#)
[John McLean](#)
 - [Still another appalling web security story](#)
[Identity withheld](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ First real Y2K clock problem...

Peter da Silva <peter@abnm.com>

Fri, 31 Dec 1999 08:32:53 -0600

The Australian Y2K readiness news page

<http://203.2.193.77/news-index.cfm.htm>

seems to have a clock problem. I was checking it as the time change swept over Australia, and it "hung" at 23:56:15 for quite a while. I quit watching it about half an hour later. I just checked it again and it's lost over 15 days: The "last update" just jumped back to 15 Dec 1999, 00:23.

I wonder what the cause is? One of my co-workers has noted that other web pages are having similar problems.

✶ Whoops! Auckland Awkward Awk! (From Dave Farber's IP)

John Wharton <jwharton@netcom.com>

Fri, 31 Dec 1999 10:47:06 -0800 (PST)

The Auckland (N.Z.) International Airport has a web site to keep the public informed on Y2K issues (www.auckland-airport.co.nz/airport_newsflash.html).

This morning they issued a "News Flash" stating that "the airport is operating as normal. No Y2K problems have been experienced and all operations are continuing as usual."

The News Flash is time-stamped "02:58 1 Jan 100".

--John Wharton

[Y2Kudos to Dave Farber, whose IP distribution is often full of RISKS items. This time his recent mailings have been chock full of fresh Y2K items. Dave, MANY THANKS, and Happy New Year to all of you! PGN]

✶ Game Over at end of millennium... (via Dave Farber's IP)

"John Elsbury" <john.elsbury@clear.net.nz>

Thu, 30 Dec 1999 09:32:21 +1300

I just have to share this... From NZ Herald, December 30 1999:

"The Waitakere City Council (West Auckland, New Zealand) has fixed an embarrassing glitch in a millennium clock in Henderson that flashes a message

telling people to be Y2K-prepared. In a test run on the clock, donated by a Korean couple, officials discovered that the message would have changed to "GAME OVER" at midnight on New Year's Eve."

Do they know something we don't? Shades of that Arthur C Clarke story about the names of God...

By the time this appears we will know.

✦ Credit-card machines in U.K. confused by Y2K

"NewsScan" <newsscan@newsscan.com>
Wed, 29 Dec 1999 07:42:56 -0700

Because central computers doing four-day diagnostic checks were unable to recognize the year 2000 as a valid date, as many as 20,000 credit card machines in England failed to allow merchants to "swipe" the cards through the machines during recent holidays, forcing the data to be entered manually and causing shopper delays. The machines are manufactured by Racal Electronics and supplied to merchants by HSBC, a bank holding company. A Racal executive says, "It is a software and date-related issue, which will be resolved and we're entirely confident that terminals will revert to full functionality at the start of the New Year."
[Reuters/*San Jose Mercury News*, 29 Dec 1999;
<http://www.sjmercury.com/svtech/news/breaking/reuters/docs/359901.htm>
NewsScan Daily, 29 Dec 1999, reproduced with permission]

⚡ IP: Y2K claims early victims (from Dave Farber's IP)

"John Locke-Wheaton" <john.locke-wheaton@bigfoot.com>

Wed, 29 Dec 1999 12:58:45 -0500

In the UK yesterday 20,000 machines in shops across the UK were reported to be rejecting all credit cards as customers tried to pay for goods. The reason? The settlement date is four days later - January 1, 2000 and so the set of transactions that make up the credit payment crosses the date changeover. The problem may disappear in four days time, when the entire transaction set will be within the new millennium.

Like most bugs, it is totally understandable and - given hindsight - totally predictable. As will be all the other Y2K problems that creep out of the woodwork. Let's hope that none of the other bugs are life threatening.

john.locke-wheaton@bigfoot.com +44 (0) 7044 011 532

⚡ Pentagon Y2K preparations

Dave Stringer-Calvert <dave_sc@csl.sri.com>

Fri, 31 Dec 1999 11:54:16 -0800

DefenseLINK, the Pentagon's main Web site, was intended to keep the public assured that Y2K was a nonproblem for DoD. However, the site was accidentally disabled on 30 Dec 1999 when other sites were taken off the Net to guard against cracker activities. The process of restoring

service was hindered by admins corrupting the domain name server. [Source: PGN-ed from CNN <http://www.cnn.com/1999/TECH/computing/12/31/y2k.reports.roundup.01/index.html>]

🔥 Oakland CA 911

John Wharton <jwharton@netcom.com>
Wed, 29 Dec 1999 10:47:58 -0800 (PST)

[This item is retitled and adapted from the IP list of Dave Farber <farber@cis.upenn.edu>.]

KCBS radio is reporting this morning that the Oakland 911 Emergency call system has determined its call prioritization algorithm is, well, technically speaking, /not/ fully Y2K compliant yet.

Apparently incoming calls are timestamped with just a two-digit year code. Normally the call routing software gives top priority to the oldest (=earliest) calls, as one would expect.

Alas, this means that as of the Friday midnight roll-over, all pending calls will instantly be kicked to the bad end of the priority list. As I interpret the news reports, the post-rollover calls will be stamped 1/1/1900, and, naturally, anyone who "just" called -- at 11:58 Friday evening, say -- is in far less dire straits than people who have been on hold for nearly 100 years.

Oakland's solution, the 911 officials say, will be that, starting at

11:50pm or so, all not-yet-dealt-with calls will be transferred to a different phone system to ensure that they don't get lost. Dispatchers can then continue dealing with existing emergencies while newer calls queue up normally until dispatchers again become available.

(The moral? It's probably best /not/ to have an emergency in Oakland during those last few minutes before midnight...)

>=====

My first impression was that this was a terribly embarrassing oversight, for this problem not to have been "fixed" months ago. Date-stamps being processed backwards is /exactly/ the textbook example of what happens when the year field overflows.

On the other hand, it /does/ seem the problem will be terribly short-lived, affecting maybe five or ten minutes' worth of calls -- ever. After 12:10am or so, then, and for the remainder of the next century, the original call prioritization algorithms should continue to work just fine.

Whereas re-opening the program source, rejiggering the code, augmenting the data structures and so forth could quite plausibly introduce new problems and incompatibilities that might bedevil emergency call processing for months.

Leading one to wonder: was this just an embarrassing oversight? Or a deliberate, rational cost-benefit decision to leave sleeping codes lay?

--John Wharton

[Note added later in Dave Farber's IP from John:
(If) unchecked, this WOULD have been a most-life-threatening oversight.]

⚡ Two possibly unaddressed Y2K problems (From Dave Farber's IP)

Brett Glass <brett@lariat.org>

Thu, 30 Dec 1999 16:52:36 -0700

While performing a Y2K check of a client's computers, I discovered a small program, written in BASIC, which suggests an entire class of potential Y2K glitches which has not been publicized and may plague us on or after January 1, 2000.

In the client's back office was an older PC attached to a modem. Each time the computer was booted, it ran a simple program which instructed the internal modem to make a brief telephone call to a telephone number somewhere in Colorado. Upon connecting, the computer received the date and time, set its clock accordingly, and then hung up.

Inspection of the program revealed that it received and used only two digits for the year.

What number was the computer calling? After a bit of snooping on the Internet, I discovered that the number was that of the Automated Computer Time Service (ACTS), provided by NIST (the National Institute of Science

and Technology, previously known as the National Bureau of Standards). The time message received by the program, derived from an atomic clock, looks like this:

```
JJJJJ YRMODA HH:MM:SS TT L DUT1 msADV UTC(NIST) OTM  
where
```

JJJJJ is the Modified Julian Date (MJD);

YRMODA is the date (two digits each for year, month, and day);
and

HH:MM:SS is the time in hours, minutes, and seconds.
(The remaining fields are documented online at
<http://www.bldrdoc.gov/timefreq/service/acts.htm>.)

What is interesting is that the BASIC program provided by the NIST itself (the same agency, ironically, which distributes the Malcolm Baldrige quality awards and offers Y2K help to small businesses) ignored the Julian date and used only the two-digit year to set the computer's clock. This software was posted on the Internet by the NIST until approximately last October.

While ACTS can be used in a Y2K-compliant manner, the way to do this is somewhat arcane (few programmers understand the concept of a Julian date, and conversion is tedious). Perhaps this is why the NIST's own software -- which was doubtless used verbatim or as the basis for other programs -- cut corners, as most programmers were likely to do, and used only the two digit "YR" code for the year.

According to the NIST's ACTS Web page (<http://www.bldrdoc.gov/timefreq/service/acts.htm>), more than 10,000 computers call the NIST's number each day. How many are running that old

BASIC program, or similar ones published on computer bulletin boards, in magazines, or on the Internet, which have the same flaw?

But wait.... It gets worse. Apparently, the time code transmitted by ACTS is similar to that used by the NIST's radio stations --WWV, WWVH, and WWVB -- to transmit time and date information the entire world. WWV's binary coded decimal format, described on the Web at http://www.boulder.nist.gov/timefreq/pubs/sp432/s_appb.htm, also uses only two digits for the year. Worse still, the Julian date is not present, so there is no way, using this code, to distinguish between the years 1900 and 2000.

Alas, some digital logic circuits which interpret the codes from WWV, WWVH, and WWVB are literally hard-wired to the existing format. (According to some quick research I've done on the Net, these range from an old Heathkit called "The Most Accurate Clock" to laboratory instruments to traffic signal controllers.) So, the NIST does not have the option of changing the format to include a 4-digit year for fear of breaking this equipment. Unfortunately, it is unclear whether owners of this equipment are aware of the potential problems in these embedded systems -- some of which, again, use hard-wired digital logic rather than microprocessors. Will traffic signals in Los Angeles and Orange County, which are said to use WWV as a time standard (<http://www.odetics-its.com/showcase/TASK2-2/la.html>), fail? Or will they become confused about the day of the week and snarl traffic by using "weekend" timings on a weekday, or vice versa?

What other municipal, scientific, or military embedded systems will go awry because they rely on the NIST's 2-digit time codes?

Ironically, while the NIST Web site contains an article (<http://www.nist.gov/y2k/embeddedarticle.htm>) warning users to evaluate embedded systems for Y2K compliance, I have been unable to find any article in which the NIST mentions the format of its own time signals as a potential source of Y2K problems. Today, when I used the "Advanced Search" facility on the NIST's Web site to search for the call sign "WWV" together with the term "Y2K" or "2000," it failed to turn up any hits whatsoever. The NIST's Y2K compliance page, at <http://www.nist.gov/y2k/nistcomp.htm>, lists both ACTS and the agency's "time synchronization" services as Y2K compliant.

Conclusions are left as an exercise for the reader.

--Brett Glass

⚡ Low-tech Y2K failure

"Earl Truss" <etruss@sprintmail.com>

Sun, 26 Dec 1999 16:27:10 -0600

[Source: Bank blames error on printing vendor, Dee DePass, *Minneapolis Star Tribune*, 21 Dec 1999; PGN-ed]

Wells Fargo & Co. sends out a batch of renewal notices - dated 1900

Wells Fargo & Co. experienced its first public Y2K glitch last

week when it mailed 13,000 certificate-of-deposit renewal notices with the year 1900 on them. The bank said the notices told customers in 10 states that their certificates would expire in January 1900 instead of January 2000. It isn't known if any Minnesota customers received the letters. Wells spokeswoman Teresa Morrow said the error was attributable to a statement-printing vendor who forgot to change the date on its printing machines. Morrow said Wells sent statements to the printer that said 1/15/00 and the vendor mistakenly translated the 00 as the year 1900. The mistake was discovered Dec.13, and officials immediately sent out letters apologizing for the error. Customers were told they would receive revised renewal notices in a few weeks. Morrow said, "We asked [the printer] if it was Y2K related and they said, 'It was just us not setting our date on our printer.'" Morrow said she didn't know if the mistake would alter Wells' relationship with the vendor. She added, "If that is the worst thing that happens to us with Y2K, then we will be set for life." Still, observers called the error an embarrassing blow to a company that just last week declared it and its critical suppliers were ready for Y2K, after having tested all its computer systems three times. Federal regulators and the Minnesota Bankers Association have repeatedly said all banks in Minnesota are ready for Y2K and don't expect any problems. Even so, Wells Fargo and its competitors are staffing technical command centers for four or five days after New Year's Eve, just in case a more

serious glitch occurs. While most banks will be closed for the New Year's Day holiday, many will have technical staff in the branches checking on lights, heat and computers.

The risks: not testing the low-tech procedures for updating date information -- "Well, we never changed that part of the date before."

⚡ Risks of expiring digital certificates in older Web browsers

David Tarabar <dtarabar@worldnet.att.net>

Wed, 29 Dec 1999 10:16:09 -0500

> Millions of people using older versions of Netscape and Microsoft Web
> browsers may not be able to access some personal finance and e-commerce
> sites starting January 1. It won't be due to the dreaded Y2K
> bug. Instead, it's because electronic credentials embedded in
> browsers are
> set to expire on Dec. 31 at midnight.

This is the lead of an article in the **San Jose Mercury News** on 29 Dec 1999, which warns that secure transactions may fail or be blocked because of expiring digital certificates. Many banks are posting warnings to their customers, warning that they need to update their net browsers, and SOON !!

Microsoft's Internet Explorer for Macintosh only discovered this problem in the last three weeks and posted a fix on Dec 21.

I especially enjoyed this quote:

> Ben Golub, VeriSign's director of Internet marketing and sales, said the

> Dec. 31 expiration date was chosen about five years ago
because at the
> time browsers couldn't accept dates beyond 1999.

> "In retrospect, maybe we should have chosen December 15," he
said. "It's
> just an unfortunate timing kind of thing."

⚡ Shirley you can't mean this date is bad!

"Conrad Heiney" <conrad@fringehead.org>

Thu, 30 Dec 1999 15:07:09 -0800

There are multiple risks, apparently, involved with multiple
types of dates.

Experts said early efforts focused on checking dates --
typically identified

with a heading "mm-dd-yy" or "date" -- buried within computer
code. But

prankster programmers sometimes used unusual nomenclature that
can make

these date variables nearly impossible to find. Data Integrity
said it

found a date field called "Shirley" when it reviewed software at
a major

bank in the Northeast, which it declined to identify. The
programmer

responsible, it turned out, was dating a woman named Shirley
when he wrote

the software. [Source: The Year 2000 Challenge, *Wall Street
Journal*, 30

Dec 1999]

⚡ The risks of last minute Y2K patches

Matt Blaze <mab@research.att.com>

Fri, 31 Dec 1999 01:55:01 -0500

Jane Garvey, the FAA administrator, was quoted that a late software patch was applied to her agency's critical ``HOCSR'' computers, which process flight plan and radar data for controllers. The repair was completed early on 30 Dec. Garvey said the minor problem turned up during continued testing of the agency's systems, which were declared Y2K-ready in June. ``We're continuing to test right up to the last moment. We erred on the side of caution. The patch is in. It's been fixed. It's a very, very minor issue.''

["Last Minute Y2K precautions Taken", *The New York Times*, 31 Dec 1999 <<http://www.nytimes.com/aponline/w/AP-Y2K-National.html>>]

Assuming the story is accurate, RISKS readers will undoubtedly wonder whether whatever benefits this fix might convey will be outweighed by the risks of patching a critical system the day before the very event that will trigger the execution of the patched code. Given the combinatorially explosive number of potential interactions in any complex system, it seems strange indeed to conclude that *any* change is just a "very, very minor issue". Pondering this question will certainly give me something to do on my Saturday morning flight... matt

✶ Re: Y2K fear vs. Common sense ([RISKS-20.70](#))

Scott Nicol <snicol@apk.net>

Mon, 20 Dec 1999 01:12:45 -0500

- > 1) The generator is in a hastily built wooden hut secured with a padlock.
- > The hut is located on the outside wall of our data center.
- 3,500 gallons
- > of boom.

Most large generators are diesel. I don't know if this particular generator is diesel, but if it is, diesel does not go boom, and it doesn't burn very well, either. It's about as stable as cooking oil.

Gasoline, in its liquid state, does not go boom either. It does burn pretty well, though. If you had an almost empty tank of gasoline, you could have enough vapor that it might go boom.

I'm not a chemical engineer, so check this with other sources if you like.

Scott Nicol <snicol@apk.net>

[Lots of you commented on this gaffe. PGN]

⚡ Re: Y2K Fear vs. Common Sense ([RISKS-20.70](#))

Eric Roesinger <eric@erie-pr.com>

Thu, 30 Dec 1999 18:15:59 GMT

- > All of our upper management is absolutely terrified of the end of this
- > year. They are convinced that there is going to be a major disaster
- > at the stroke of midnight.

Would it frighten them any more, to know that power companies generally operate on GMT?

The risks of failing to understand this necessity of managing a power grid connecting multiple utilities and spanning several time zones, are:

- + presumption of more time for disaster preparation, than actually

 - exists, should fears be justified; and

- + hysteria over impending doom, after the possibility of its occurrence

 - has passed, should fears be unjustified.

I keep telling people where I live, that they can stop worrying about

their electric power, shortly after 7PM. West of here, people can stop

worrying even earlier (4PM in California, for example).

Even if a few generating facilities did fail, unless they lost station-

keeping power, those facilities would remove themselves from the grid,

immediately. As far as I know, it's become standard practice to have

battery-backed station-keeping power, since a station without it caused

a major regional blackout in the Northeastern US, some years ago.

(Either their backup generator failed while the others were down for

maintenance, or vice versa; I don't remember. The story comes second-hand

from a former colleague, who, at the time, worked at a nearby manufacturing

plant, whose generators were used to provide the power to bring the station

back online.) [...]

✶ Abolishing leap-seconds

Rob Seaman <seaman@noao.edu>

Tue, 21 Dec 99 17:13:33 MST

Various issues involving leap-seconds have been discussed in RISKS in the past. One of the most creative was "Length of Day & Reservoirs" by Scott Lucero in [RISKS-17.87](#), suggesting that we might avoid future leap-seconds through calibrating the Earth's actual rotation rate by selectively filling reservoirs. (Some mechanism would be needed for recalibrating the Earth once the reservoirs were full...)

The time and frequency community is in the early stages of considering a proposal to simply stop issuing leap-seconds. (Alternatives are also being considered.) There has been some rousing discussion of this in `comp.protocols.time.ntp` and `sci.astro.fits` (among others).

Possible risks include Y2K-style risks of software and firmware relying on $|\text{UTC}-\text{UT1}| < 0.9\text{s}$. More fundamentally, this would be a change to the original design requirement of UTC that ties clocks around the world to our most visible standard of civil time - the Earth itself. The general risks are similar to other small communities that control technical resources (for instance, utility companies) used by virtually everybody. The effects of overtly minor operational changes are highly non-linear and can be magnified immensely.

For a sense of the scale of the change, a century of leap-seconds is about equal to half the width of the sun or the moon on the sky. This is enormous for some purposes, negligible for others.

Should we take comfort or dread that the metrologists are debating this issue with Y2K looming?

Rob Seaman

✶ Is the connection secure or isn't it?

Don Byrd <dbyrd@cs.umass.edu>
Mon, 20 Dec 1999 16:45:26 -0500

A month or so ago, I was trying to order plane tickets via the Travelocity Web site, when I noticed that--though the page I was looking at prominently claimed to be "secure", and even had a link to click on where they explained in detail why it really did protect your privacy--Netscape (4.5 for Windows) didn't agree: the little lock icon on the bottom was open! I asked for Page Info, and that confirmed that the connection was not secure. Needless to say, I didn't go ahead with the purchase.

Much more recently, I was trying to order a CD from the U.S. Public Radio Music Source (www.75music.com) when what appeared to be the same thing happened. But this time Page Info showed the connection was secure, and I went ahead and gave them my credit card info.

The RISK? Presumably the chance of outsiders seeing your

confidential information because what you assumed was a secure connection really wasn't. Of course one should never trust a Web site's statement that the page you're viewing is secure, but if it's an outfit as well-known and reputable (as far as I know) as Travelocity, I'll bet a lot of people will assume it is--especially if they explicitly tell you how they're protecting your confidential information, as this page did.

My experience also raises the question as to whether you can even trust the browser to tell you if you have a secure connection; I sure hope so, at least if JavaScript is disabled (I seem to recall the Princeton group pointing out that JavaScript can take over the browser's UI almost completely).

Don Byrd, Center for Intelligent Information Retrieval (CIIR),
Computer Science Department, UMass, Amherst, MA 01003 dbyrd@cs.umass.edu
413-545-3147

Privacy broken by Sanity.com

John McLean <john.mclean@ubs.com>
Wed, 29 Dec 1999 14:02:33 +0100

Sanity.com, the Australian company who keen readers will remember as allowing purchases of CDs without payment ([RISKS-20.68](#)), have stuffed up again, this time sending all their customers an e-mail that included the

e-mail addresses of more than 140 of its customers. This violated their own stated privacy policy. [Source: Fairfax newspapers - *The Age* and *Sydney Morning Herald*, PGN-ed from John McLean, Zurich, Switzerland; <http://www.it.fairfax.com.au/e-commerce/19991222/A52132-1999Dec22.html>]

⚡ Still another appalling web security story

<[Identity withheld]>

20 Dec 1999

A friend recently asked me to join an online "community" which he had created on a service called Intranets.com (<http://www.intranets.com/>). There was some sort of verification code to enter, then I was asked to create an account, including a username and password. I went ahead and did so.

To my utter surprise, I then received an e-mail message from welcome@intranets.com containing the login and password I had provided!

The risk is clear. Electronic mail is an inherently insecure medium, both because of the way it is generally stored and because it is transmitted as clear text over TCP/IP networks. Not only is the security of an account on Intranets.com jeopardized by this practice, but if someone should use a password which they already use for other services, then their other accounts are also at risk.

Intranets.com does have a privacy statement, including a section

on security, but there's nothing there which would lead one to believe that the company would do something like this.

The lessons for users? First, when signing up for a service, never use a password which you wish to keep secret. If you wish to have a consistent password across sites (itself a risky practice), you should change the password after you've signed up. And even then, you should probably perform an experiment to make sure the site isn't so daft as to send you a copy of your changed password in the e-mail.

The lesson for developers? Security mustn't be so difficult to use that users and website owners are tempted to defeat it by practices such as reusing passwords and sending them over e-mail. The answer may lie in something like the digital keychain which I've read is contained in MacOS 9. However, unless there's a way to take your keychain with you (on a disk, card, etc.) or to access it from a central location (via a trusted keychain storage site), this will only work for people who access the web from one computer.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 72

Sunday 2 January 2000

Contents

- [Y2K early reports](#)
[PGN](#)
 - [Pentagon satellite intelligence system Y2K failure](#)
[PGN](#)
 - [Re: Y2K](#)
[Derek Tam](#)
 - [Re: Y2K goofs](#)
[matt](#)
 - [Y2K risks comment](#)
[Rebecca Mercuri](#)
 - [Y2K kills Toronto bus information service](#)
[Mark Brader](#)
 - [Y2K warning software is wrong!](#)
[Jeremy Epstein](#)
 - [Re: Y2K fear vs. Common sense](#)
[John Palkovic](#)
[William Ehrich](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Y2K early reports

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

Sun, 2 Jan 100 12:45:47 PST

On the whole, Y2K came and went without major immediately noted problems.

Predictions still abound for deferred problems. In this message, I have attempted to summarize in one place some of the reported Y2K weirdnesses.

There are a lot of lessons that should have been learned from the entire process, but we'll address those in this forum later on after a little more time to reflect. My preliminary conclusions are not surprising: there has been a pervasive lack of foresight, generally lousy software engineering, overemphasis on the remediation process without deeper understanding, ignoring the risks of remediation by potentially untrustworthy third parties, and so on.

Dave Stringer-Calvert <dave_sc@csl.sri.com> has been monitoring CSL's Y2K compliance. I have adapted the following items from his e-mail to me:

[PLEASE note the Date: field on this message. This is apparently a widespread problem. In my case, it seems to be a lurking Y2K noncompliance in the Columbia MM that I have been using for so many years.]

QuidProQuo 2.1.2 web servers for Macs are returning 1-Jan-100 as the date to client queries...

Dave's favorite "The Yorkshire Evening Press" at <http://www.>

thisisyork.co.uk

claims a date of "Saturday, January 1, 100".

Also <http://www.kfrc.com/> [That's some old chicken!]

Also an ELM 2.4 problem (noted by Leo Taiariol <leot@iphase.com>)

On 2 Jan, www.cowsnet.com/home.html gave Sunday, 2 January 100

www.kpix.com/tv/schedule.html

gives:

```
Error: cannot open /ht/tv/schedules/January-1-19100
```

[Dave sent me this at Fri, 31 Dec 1999 19:39:43 -0800:]

GO to www.npl.co.uk/cgi-bin/countdown.pl NOW!!!!

It reads "31 Dec 1999 26:39 UTC"

[Not only an incorrect atomic clock, but **WRONGLY** incorrect!

18:39 PST + 8:00 time shift = 27:39, not 26:39 UTC!

[It has now been repaired. PGN]

Various sites have been hacked, including

www.dea.com

["Look mom I hacked dea.comm!!! y2k crew is here. hacked by miloco.]

www.core.net

There is some lovely Y2K humor on www.2600.com .

On 2 Jan, <http://www.giga-byte.com/gigabyte-web/newindex.htm>

(they manufacture motherboards) has the date as Jan 2 2100.
The javascript function is:

```
// standard date display function with y2k compatibility
```

```
function displayDate() {  
  var this_month = new makeArray(12);  
  this_month[0] = "January";  
  this_month[1] = "February";  
  this_month[2] = "March";  
  this_month[3] = "April";  
  this_month[4] = "May";  
  this_month[5] = "June";  
  this_month[6] = "July";
```

```
this_month[7] = "August";
this_month[8] = "September";
this_month[9] = "October";
this_month[10] = "November";
this_month[11] = "December";
var today = new Date();
var day = today.getDate();
var month = today.getMonth();
var year = today.getFullYear();
if (year < 100){
    year += 1900;
}
else{
    year += 2000;
}
return(this_month[month]+" "+day+" ", "+year);
}
// -->
```

The flaw is beautifully obvious. The comment is wonderful.

<http://www.wfs.org/futurist.htm>

Time left to January 1 2000:
-1 years, 11 months, 29 days, 14 hours, 21 minutes, 45 seconds
and counting... It's actually correct, in a strange sort of way.

[Jeremy Epstein has another manifestation of this problem,
below. PGN]

On 2 Jan, the Australian online media news gateway www.pressrelease.com.au,
gave the date as
3 Jan, 3900
and www.happypuppy.com gave 01/2/20100

[http://www.amazon.co.uk/exec/obidos/ASIN/B00002716Z/
qid=946835401/sr=1-6/026-4578278-4117058](http://www.amazon.co.uk/exec/obidos/ASIN/B00002716Z/qid=946835401/sr=1-6/026-4578278-4117058)

claims a Sonic Youth CD will be made available 10 Oct 2011.

Thanks to Dave. Also his colleague Mike Hogsett noted that
<http://www.startrekcontinuum.com/brf/VOYUpcomingtop.asp>
shows the next Star Trek Voyager episode has a first air-date of
1/1/1900.

Mike also noted that www.abc7news.com had Jan 1 100.

John Murrell observed the US Naval Observatory calendar at 19,000.

Andrew Koenig spotted the New York Times Website, January 1, 1900.

⚡ Pentagon satellite intelligence system Y2K failure

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

Sun, 2 Jan 100 10:13:12 PST

As the Pentagon folks were claiming that everything was working fine, a computer system processing satellite intelligence data lost its data collection ability at 7pm EST (midnight GMT) on Friday evening for about 2.5 hours. [Source: Pentagon Withheld News of Major New Year's Computer Failure, by Roberto Suro, *The Washington Post*, 2 Jan 2000, A8.]

⚡ Re: Y2K

Derek Tam <dtam@derekweb.com>

Sun, 02 Jan 2000 14:48:01 -0500

I'm sure someone else will have pointed out the cause of this problem by now, I had a first hand experience with it. Script-generated dates using the `localtime()` function return a list of values, the current month, day, hour, minutes, seconds, and year. A common misconception is that the

(former) 2-digit year value is just that: a 2-digit year, when in fact it is the number of years elapsed since 1900. So when we hit Jan 1, 2000, the year value became 100. So now we are seeing some fairly interesting dates such as Jan 1, 100 and Jan 1, 19100 (or 20100) for those who were prepending the "19" to the year value. The correct way to resolve this is of course
 $\$year = 1900 + \$year.$

Derek Tam Skwid? <<http://www.derekweb.com/>>

✶ Re: Y2K goofs

Matt <matt@redcat.org.uk>

Sat, 1 Jan 2000 04:29:45 +0000

Just a few goofs I spotted on the graveyard shift today.

Many little websites - localtime error, pretty common, where someone had misunderstood the value returned (current year, minus 1900) and assumed it meant "2 digit year". Prefix it with 19 and we get "current date: January 1, 19100"

www.apple.com - localtime error, by someone who at the stroke of midnight GMT conveniently updated their code to change the prefix from "19" to "20" having presumably audited their code. Ooops.

The claim on their main page over their very prominent Y2K statement that the date was "January 1, 20100"

Compaq's site somehow managed to claim it was January the 2nd.

Sun's "Y2K readiness countdown" told me the time was "0-6:53:23
January 1
2000" although I suspect this may be a seriously broken effort
at converting
their value (american somewhere) to my localtime (GMT). This was
viewed on a
sun, using netscape. The time at that point was just gone
midnight.

And you already know about the Auckland airports fantastic 100AD
jumbo. I
have to wonder if the civil aviation authority permits 1900 year
old
aircraft to make such long flights. ;)

The risk being highlighted? well, a large number of these
problems are
simply firms making themselves look stupid in their rush to
highlight how
Y2K aware they are.

Here? Well, I can't tell you where "here" is, but we had a
serious
alert level raised at one point... for a dead fuse.

The fireworks were nice ;)

matt@redcat.org.uk - - --> <http://www.redcat.org.uk/~matt/>

Y2K Risks Comment

Rebecca Mercuri <mercuri@gradient.cis.upenn.edu>

Sat, 1 Jan 2000 23:33:19 -0500 (EST)

Since the world's computers didn't all crash on 1/1/00, some
newscasters
have needed to find a way to share their angst with the public.
Today I
heard a reporter complain about the \$XB "wasted" on solving the

Y2K bug,
with the speculation that it was a ploy by the computer industry
to get
extra income. I wonder if we spent \$NB on preventive health
care and nobody
got sick, if the news media would consider that also a waste?

As for myself, all of the billing systems I'd authored back in
the early
1980s that weren't Y2K compliant were thankfully retired by 1998
(still a
lot longer than I'd expected they'd continue to have been
used). I did get
a call at 11:30AM (EST) from an old client with an old 486PC
that seemed to
have reset its date to January 4, 1980. After using the Date
command with
01-01-2000 everything seemed to be fine. (No, I didn't charge
them.)

A Happy (and Profitable) Y2K to All, Rebecca Mercuri
<mercuri@acm.org>

✶ Y2K kills Toronto bus information service

Mark Brader <msb@vex.net>

Sat, 1 Jan 2000 16:22:49 -0500 (EST)

It was possible from 1987 to 1999 to phone a number posted on
each bus
stop in Toronto and hear the scheduled time of the next two or
three buses.

The TTC determined some months ago that this system was not Y2K
compatible
and was also under-used; so as of today, it's been withdrawn
indefinitely.

See <http://www.ttc.ca/postings/gso-comrpt/documents/report/f591/_conv.htm>.

Mark Brader, Toronto <msb@vex.net>

[Mark likes PGN's old RISKS quote:

"This problem gives new meaning to "going out on a date"]

⚡ Y2K warning software is wrong!

Jeremy Epstein <jepstein@monumental.com>

Sun, 2 Jan 2000 07:15:30 -0500 (EST)

I run McAfee Office 2000 on my home computer, which includes McAfee WinGauge.

That's a little gizmo with four panels: the CPU usage, memory usage, DOS

memory usage, and "days to Y2K". This morning (January 2nd), the days

to Y2K reads "1", which I suppose is correct in an unusual sense of the

term. But the time remaining to Y2K is -7:-18:-55 as I write this. While

I'll agree that January 1st ended about 7 hours and 20 minutes ago, I

wouldn't normally expect to see that written as -7:-18:-55!

Of course, this isn't mission critical, but it is a rather strange symptom

for software that's supposed to be providing a countdown...

--Jeremy Epstein, jepstein@acm.org

⚡ Re: Y2K fear vs. Common sense ([RISKS-20.70](#))

John Palkovic <palkovic@lucent.com>

23 Dec 1999 11:33:40 -0600

Ironic that "Common sense" is mentioned in the subject of this message.

I think someone has been watching too many Hollywood movies. Fuel in tanks does not explode spontaneously; it needs to be mixed with a greater volume of air and ignited. This is a continuous process in a gasoline motor. Fuel tanks can burn, but they don't explode too well (excepting Ford Pintos).

The risk here is that someone has not checked their facts and is spreading fear and panic. It seems that in the case of Y2K, the greatest thing we have to fear is fear itself.

-John

[Also commented on by Mike Ellims. PGN]

⚡ Re: Y2K fear vs. Common sense ([RISKS-20.70](#))

William Ehrich <ehrich@minn.net>

Mon, 20 Dec 1999 13:25:45 -0600

> We would not survive the loss of our data center.

Common sense might suggest backing up your data. Off campus.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 73

Monday 3 January 2000

Contents

- [Palm Springs airport radarless for almost two weeks](#)
[PGN](#)
- [Y2K fix cost?](#)
[Don Cleghorn](#)
- [New Year's Eve 11pm news repeated hourly in NZ: 99 > 00](#)
[Callum McKenzie](#)
- [Nokia phone not Y2K compliant?](#)
[Jari Takkala](#)
- [Effects of Y2K on mobile and telephone networks](#)
[Jari Takkala](#)
- [Year 97,98,99,100](#)
[Robert Rathbone](#)
- [Y2K Filemaker Pro](#)
[Mary Shafer](#)
- [Word Perfect 5.1 and medical transcription ALL over](#)
[Don Taylor](#)
- [X-10 controller not Y2K-ok](#)
[Andrew M Greene](#)
- [Timely updates and Y2K nuclear-plant glitches](#)
[Doneel Edelson](#)

- [Disregard those OS Upgrade error messages; they're OK!](#)
[Michael Cook](#)
 - [Interesting Win95 Y2K bug?](#)
[Roger Galliett](#)
 - [Risks in poor library design](#)
[Ben Elliston](#)
 - [Unix98 localtime](#)
[John J. Francini](#)
 - [Re: Giga-byte Javascript Y2K](#)
[Kai Birger Nielsen](#)
[Andrew Fleisher](#)
 - [Javascript considered harmful](#)
[Martin Minow](#)
 - [Microsoft MSIE Y2K Insanity](#)
[Andrew D. Fernandes](#)
 - [California DMV Y2K snafu](#)
[Cliff Sojourner](#)
 - [Y2K FTP problem](#)
[Amos Shapir](#)
 - [Y2K funny computer error in Talking Clock](#)
[Bruce Stein](#)
 - [Y2K compliant? Not possible!](#)
[Fred Cohen](#)
 - [Re: Time left until Y2K](#)
[Daniel Norton](#)
[Matthew Byng-Maddick](#)
 - [Info on RISKS \(comp.risks\)](#)
-

🚨 Palm Springs airport radarless for almost two weeks

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

Sun, 2 Jan 100 17:00:08 PST

The Palm Springs radar system was seriously undependable in December, and was finally shut down for almost two weeks by the FAA.

Controllers could not track planes below 8000 feet via radar, and resorted to radio and visual contact. The FAA of course said there were no safety problems (presumably because of much wider spacing of planes -- one plane at a time in 30-mile regions). Nevertheless, at least 15 incidents of avoidance based on cockpit warnings were reported in 11 days. Two cases involved distances of about 400 feet, both involving smaller aircraft near commercial planes. [Source: *Los Angeles Times*, 31 Dec 1999; PGN-ed]

[I have a bunch of other non-Y2K stuff pending. Please be patient.]

⚡ Y2K fix cost?

"Don" <don@globility.com>
Mon, 3 Jan 2000 09:16:56 -0500

Now that the media is ranting about the \$600 billion "down the drain" (CBC radio this morning), it makes me wonder what would the cost have been to build everything Y2K-compliant from the start (assuming perfect foresight)? And what would that cost be in year 2000 dollars?

Don Cleghorn don@globility.com

[For those who think money was wasted, it is intriguing to see how messy the situation was as recently as six months ago. There has been some real progress, which probably never would have taken place in the absence of the Y2K hype. But the old technique for keeping

elephants

away probably would not have worked. (See, there are no elephants!) But,

it was nice to see that there was not much panic, as Paul Saffo pointed

out in a KCRW radio show we were on in L.A. a few minutes ago.) PGN]

🚩 New Year's Eve 11pm news repeated hourly in NZ: 99 > 00

Callum McKenzie <callum@physics.otago.ac.nz>

Mon, 3 Jan 2000 14:01:13 +1300

At 9pm on 1 Jan 2000, I turned the radio to a local station in Dunedin, NZ

to hear the news reader announce the time to be 11 o'clock. As I continued

to listen I realised that the news being read was from the previous evening.

At 10pm the same news was re-read. It would appear that a computer, either

at the radio station or at their news supplier, was trying to play the most

recent tape based on a 2-digit year.

The risks are obvious, confusion about both the time and the news, and a

lack of information about what really is happening in the world. The real

irony was that the lead story was about an expected lack of Y2K problems.

Then again maybe its a cunning strategy to avoid Y2K by never quite getting there.

[Too bad it was not in Australia or Austria. Then it might have been an

Austrich sticking its head in the sand to pretend that Y2K had

not yet
arrived. PGN]

⚡ Nokia phone not Y2K compliant?

Takkala <takkala@netwave.ca>
Sun, 2 Jan 2000 23:02:59 -0500 (EST)

Shortly before midnight on 31 Dec 1999, at about 11:15 PM, I switched my Nokia 6188 cell phone on. Having enabled the Field Test menu on the phone (enter the code: *3001#12345#), I went to Field Test screen 07 to view the current date and time. Instead of displaying "Dec 31, 1999", the screen was flashing and read out "On 71, 1999" with the correct time printed below. At midnight the year correctly switched to 2000, but the display continued to flash "On 71, 2000". This behaviour continued until Saturday night, (Jan 1 2000), when I switched the phone off and back on a few minutes later. For a brief moment the Display read "Jan 01, 1980", then "Oct 27, 1990", and finally "On 71, 2000".

After leaving a movie at 12:45 AM Sunday morning, I switched my phone back, and the display did not flash, instead it said "Jan 01, 2000", that seems fine, except that it was 2nd, not the 1st. My phone still seems to think that it is the 1st on this Sunday night.

It should be noted that a friend of mine who purchased the same phone around the same time I did (June 1999) was seeing the same behaviour. Whereas a

friend who purchased the same model phone in early December did not see any of the above strange behaviour.

Finally, pressing MENU - 8 to view the Calendar works fine. Leaving me at the current date.

Version information: (Field Test screen 61)

Nokia 6188, 430SD3a2.nef, 05/18/1999, NSD-3AX

If anyone could shed any light on this strange glitch, please post a reply.

[to Jari, please. Kiitos. PGN]

- Jari Takkala

⚡ Effects of Y2K on mobile and telephone networks

Takkala <takkala@netwave.ca>

Sun, 2 Jan 2000 23:28:09 -0500 (EST)

It seems that little has been discussed about Y2K outages resulting from telephone systems being overloaded as midnight passed around the world.

Here in Toronto, Bell Canada warned about not picking up our telephones shortly after midnight to check for a dial tone, as everyone doing so may overload the system. Well, looks as if many did not heed the warning (myself included).

The cellular networks here were extremely overloaded, resulting in fast-busy signals or silence up until about forty-five minutes past midnight. Calls

to 611 (phone service and client care) to check my cellular bill would go through, but instead of the usual voice prompts, I was greeted with a message along the lines of "Due to the unusually high volume of calls we are currently experiencing, there is a long waiting period for a service rep...".

I did not get a chance to make any calls on the landline, but a friend calling 411 (Directory Assistance) had to wait for about 5 minutes before her call was answered. Another friend said he was also greeted with several fast-busy signals or silence when attempting to make calls.

Jari Takkala

⚡ Year 97,98,99,100

Robert Rathbone <rr@dragonheart.net>

Mon, 03 Jan 2000 03:29:28 -0500

We will find the most prevalent problem with the new year as being what I call the "Year 97,98,99,100" problem. These are not necessarily benign problems of display only. I became first aware of this flaw a year ago while testing software that I had out in the field and traced the problem back to the compiler date kernels. I found that the Borland kernel (which is licensed from MS, the foundation classes) and the MS kernel was flawed. When I discovered this problem I was stunned to see such poor programming come from MS or anywhere else. I was only able to test Borland and MS

compilers because they were the ones we used in house here, though I suspect the problem might be more wide spread.

I did research and I did find MS acknowledging the problem in the first few days when they posted Y2K fixes in late 1998. Their web-site actually classified this problem as severe and could cause data corruption. What was interesting is that this problem disappeared from its predominate placement on the Y2k page within 3 days after its posting. I was alarmed when I realized that ALL software compiled prior to a certain date will have this year 100 problem. This means that most of all PC legacy software applications will be suddenly broken or untrustworthy and now you are indicating that non-PC systems are affected also.

The RISK categories for this problem fell into three groups of programmers:

The first group never tested to see if their program ran correctly or considered certain software no longer being used so no corrective action was taken.

The second group of which I was initially a part of, said to themselves, "I don't do any date comparison in my application so I can't have a Y2K problem. I just capture the date for display or store it with each record. No date manipulations at all." Well I was wrong but was fortunate to test for it early last year and issue a correction. This problem will crash most systems or cause erratic problems from memory corruption. I captured the date and time with each record that was created and stored it

out. Which is pretty common DP practice. For as long as I have been programming, over 28 years now, the year was always returned as a 2-digit number. Imagine my surprise when it became a three-digit year (100). This meant that the variable used to store the date which was sized at 8 characters now was being fed 9 characters, which meant that everywhere I had a date as mm/dd/yy it was now being fed mm/dd/yyyy. The third digit in the year stomps on top of whatever the following memory space variable is. Which I'll leave up to the reader to imagine all the potential problems that might happen. If you create arrays using these dates the problem just gets worse. Now your program may continue to run, but due to the nature of memory corruption it may just act erratic or hang or just continue trashing your database as you save out new or modified records. Even if you used a compiler that had bounds checking or you yourself did such, the year would still become the year 10. Why you would have been inclined to do bounds checking of this nature is beyond me. It would be like performing a check to see if there were more than 60 seconds in a minute. Does the sun rise from the east? Yes, everywhere but two points on the globe.

The third group found this problem but saw the 'fix' as just simple math, so simple that they didn't test the results of their math. This group falls into the fix makes it worse group.

The fact that there is increasing numbers of reports of the year 100

problem inclines me to believe there were a large group of programmers who just said "I don't do any date comparisons" and got caught and a lot of people doing rushed last minute faulty fixes when discovering a year 100.

Planes didn't fall out of the sky, but we just lost the reliable use of decades of older programs that has a date displayed somewhere because some idiot thought that the year after 99 was 100.

Robert Rathbone, President, Alchemedia Communications And Design, Inc.

P.S. I do have an large application written in 1991 that we thought no one would be using for more than a couple of years not concerned about any dates then. There are a dozen or so companys still running the DOS program today. We only sold maybe 20 systems of this application. The companies didn't want to pay for the programming to bring it up to date and I didn't really want to modify such a large application (150k+ lines of code). I just told them to set the date back to a year that matches the year 2000 and the same for 2001. They were happy that they could still run a very reliable program and we were happy not to go through the grief of debugging and introducing destabilizing bugs.

Y2K Filemaker Pro

Mary Shafer <shafer@rigel.dfrc.nasa.gov>

03 Jan 2000 11:53:19 -0800

I had a Y2K failure of sorts--the 24 December Y2K upgrade to Filemaker Pro on my laptop turned it into a keyed (networked) application, rendering it useless to me because there was no key access routine installed, naturally, since the computer is supposed to work unnetworked. As a result, I couldn't do my time sheet, or even print out a blank form, until I was able to find another PC that I could get on without a password.

Apparently, the set-up routine said that it would make the application keyed, but the secretary required to hustle around and update everyone's computer didn't understand what it meant and continued the application. She didn't know that laptops have to run unkeyed, but couldn't let me, who knew that, do the installation.

Mary Shafer, Lead Handling Qualities Engineer, SR-71/LASRE, NASA Dryden Flight Research Center, Edwards, CA shafer@rigel.dfrc.nasa.gov

⚡ Word Perfect 5.1 and medical transcription ALL over

Don Taylor <psu04033@oit.pdx.edu>
Sun, 2 Jan 2000 22:54:54 GMT

A significant portion of the medical transcription community still happily makes use of Word Perfect 5.1 for MSDOS, silently turning your doctor's report into bits. In sci.med.transcription someone posted a short note explaining how to confirm that the date format was set correctly

to handle
four-digit years. And many readers used this information to
check and
perhaps correct the settings.

However, after confirming that settings here were already
correct, and that
the software would correctly insert appropriate dates into
documents, I saw
that when displaying the list of files in directories it would
show the date
as "01-01-:0" Other users discovered that for other years the
date might be
";0" or "<0" or other interesting things.

Someone then posted the following note:

> According to the Corel WP5.1 web site regarding Y2K issues,
this is
> just the way the dates are displayed in File Manager. Check
out this
> URL for details:

> http://www.corel.com/year2000/wp_5_1_dos_advanced_users.htm

X-10 controller not Y2K-ok

Andrew M Greene <agreene@pageflexinc.com>

Mon, 3 Jan 2000 15:32:49 -0500 (EST)

My Y2K story: at midnight, the X-10 controller that I use to
control my
home's lights apparently froze. (I use X-10 to automatically
turn lights on
and off over the Jewish Sabbath, when direct intervention in an
electric
circuit is forbidden.) Fortunately, the kitchen and dining room
were left
in an "on" state, so we weren't left in the dark on Saturday
afternoon, and

resetting the timer seems to have unfrozen it. [...]

Not truly Y2K-related, but worth noting in Risks, was that *The New York Times* corrected a 102-year-old error in their issue numbering as of 1 Jan 2000. It appears that on 6 Feb 1898, a careless copyboy figured that the issue after 14,499 would be 15,000; since each day's issue number was "computed" by looking at the previous day's issue and adding 1, no one caught the error for over 100 years. The current "newsroom assistant" (no longer a copyboy) in charge of typing in the number each night starting wondering about whether an error had ever been made, worked out what the current number should be (using a spreadsheet program), and tracked down the gap. *The Times* reverted its issue number by 500 and "regrets the error."

⚡ Timely updates and Y2K nuclear-plant glitches

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

Mon, 3 Jan 2000 12:08:06 -0500

The Year 2000 Information Center - Year 2000 Bug Bytes

<http://www.year2000.com/y2kbugbytes.html>

has the following line:

Updated January 3, 1900 at 14:50 (UTC)

same for their page of press clippings

<http://www.year2000.com/y2karticles.html>

Updated January 3, 1900 at 14:44 (UTC)

also this:

Technology News

U.S. Nuclear Plants See Minor Y2K Glitches

(01/02/00, 9:44 a.m. ET) TechWeb

Seven U.S. commercial nuclear reactors experienced minor Y2K computer-related problems, but none affected safety systems and were quickly

fixed, government officials said Saturday. The plants saw malfunctions with

computer systems used to support physical plant access control, the

monitoring of operating data, and the calculation of meteorological data.

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

✦ Disregard those OS Upgrade error messages; they're OK!

Michael Cook <MLCook@collins.rockwell.com>

Mon, 20 Dec 1999 09:09:42 -0600

As part of becoming Y2K compliant, Windows NT machines here are being upgraded from NT 4.0 service pack 4 to service pack 5. A canned script has been made available to those who need to upgrade their PC.

Upon starting this script, I got the following message in a pop-up window:

"Wait one moment while we add you to the Local Administrators group.

You may see several errors as the process runs, this is normal, do not be concerned."

Reassuring?

Another pop-up window later in the upgrade process says:

"Part of the Update can generate errors. Please do not be alarmed."

If you get any messages that say you do not have rights to update, call the helpdesk..."

So, how can we differentiate between legitimate errors and those that we are to disregard? Or errors that mask other errors, and so on.

What the pop-up windows did **not** say, but maybe implied, is:

"Pay no attention to that man behind the curtain."

-- Michael Cook

🔥 Interesting Win95 Y2K bug?

"Roger Galliett" <rogerg@gci.net>

Mon, 3 Jan 2000 09:57:14 -0900

While attempting to copy a large .mpg file to CD-ROM today (1/3/2000), my application (Easy CD Creator) gave the following error message:

"The item "***(name omitted)***" cannot be added because the date and time is corrupt. Do you want to continue adding other items?"

Upon checking the file properties, it showed a creation date of 1/3/2000 and a last accessed date of 1/3/2000, but a modified date of 9/1/2099!!!!!!

Just offhand I would say this is a Win95 problem -- when it saw that the file was modified before it was created, the brilliant geniuses at Microsoft decided to simply say, "Oh, it must be that pesky Y2K bug -- add a hundred years -- THAT'LL fix it!"

However, for some reason, Easy CD Creator doesn't seem to be able to recognize this date as being valid.

The workaround I found was to open the huge file in an MPG editing program, and then re-save it under a new name. This normalizes all dates to the year 2000. There may be easier ways of handling this, but I haven't tried any others.

✂ Risks in poor library design (Re: [RISKS-20.72](#))

Ben Elliston <bj@cygnus.com>
Tue, 4 Jan 2000 06:44:47 +1100 (EST)

Recent postings about "Y2K" glitches detected on web sites highlights an important risk in software engineering--and more precisely, the design of libraries and APIs.

The C library function, `localtime()`, breaks a binary date representation into its component parts--these parts are collectively stored in a struct `tm`. One field of this structure that is of concern is `tm_year`, which, according to my Unix system's man page, is:

`tm_year` The number of years since 1900.

This is indeed clearly documented. But most programmers only read documentation when they can't get things to work, or they don't work as they expect them to.

Last century :-), programmers examined the value of this field, and thought, ``Oh, it's 98--this must be the year without the century portion'', and proceeded to tack "19" in front. At the same time, they would have tied a piece of string around their finger to remind them to change this to "20" at the end of 1999. (!)

I think it's probably safe to say that this aspect of the library is poorly designed. The empirical evidence is before us--many, many programmers misunderstood and subsequently misused this structure, causing widespread programming errors. If the library had been designed differently, so that the complete value of the year was kept in the structure, this would not have happened. My research suggests that the tm_year field has always been of `int' type, so the reason for using the number of years since 1900 was probably not to economise storage.

⚡ Unix98 localtime

"John J. Francini" <francini@progress.com>

Mon, 3 Jan 2000 10:56:42 -0500

The problem is that it's not so simple as that. The UNIX98 standard changed the localtime() function so that the year value is redefined to be the "year in the current century" rather than "years since 1900". On a system that has been patched to comply with UNIX98 `_after_` your suggested change was made, the code would break. It's better to use a function that gets the

current century and then adds (year % 100) to it, or gets the current
4-digit year direct from the OS. This covers more bases.

John Francini, francini@progress.com

⚡ Re: Giga-byte Javascript Y2K

Kai Birger Nielsen <bnielsen@daimi.au.dk>

Mon, 3 Jan 2000 10:34:21 +0100 (MET)

They seem to have "fixed" it now by changing the year += 2000
to year += 0; Welcome to Jan 3 100.

<http://www.giga-byte.com/gigabyte-web/newtop.htm>

Also note that older browser may well run Javascript 1.2 and so
actually
display Jan 3 2000. I wonder if they tested this on an old
browser ?

Birger Nielsen (bnielsen@daimi.au.dk)

[also noted by Finn Poschmann <fposch@cdhowe.org>. PGN]

⚡ Re: Giga-byte Javascript Y2K

Andrew Fleisher <andrew8@start.com.au>

Mon, 3 Jan 2000 21:10:11 +1100

More interestingly is that a pc I have with a giga-byte
motherboard supplies
the year 2094 on boot, even after correcting the year to 2000
and applying
the patch supplied by giga-byte.

Andrew Fleisher <andrew8@start.com.au>

⚡ Javascript considered harmful

Martin Minow <minow@pobox.com>

Mon, 03 Jan 2000 09:46:28 -0800

The Javascript Y2K bug I wrote you about yesterday is, unfortunately, uglier than I had realized: apparently, Netscape's JavaScript returns (year - 1900), while (today), Internet Explorer returns the actual year. I fixed (at least for now), my bug by writing:

```
revdate = new Date(document.lastModified);
year = revdate.getYear();
if (year < 1900) {
    year = year + 1900;
}
```

This works on the four browsers I tried today, but I don't guarantee it will work on a fifth. (Standards are wonderful: everyone should have a few).

Martin Minow, minow@pobox.com

⚡ Microsoft MSIE Y2K Insanity

"Andrew D. Fernandes" <andrew@cryptonym.com>

Mon, 03 Jan 2000 11:14:54 -0500

Uh-oh. This JavaScript snippet actually is CORRECT. As defined in the JavaScript standard, the "year" field should indicate the number of elapsed

years since 1900. What was going on?

It turns out that Fujitsu's web page displays correctly under Netscape-4.7,
but not on MSIE-5.01. I'm not sure about MSIE4.x.

The risks? It seems that Microsoft has yet-again thrown a patch into its operating system without checking for standards compliance, or doing a lot of regression testing. JavaScript's "Date" function has always been Y2K compliant; programmers often just haven't used it properly.

Andrew D. Fernandes <andrew@cryptonym.com>, Principal, Cryptonym Corporation

<<http://www.cryptonym.com>> +1 919 469 4714

California DMV Y2K snafu

Cliff Sojourner <cls@cisco.com>

Sun, 02 Jan 2000 21:57:37 -0800

The registration and stickers for a boat I own arrived in the mail 1999/12/31. the "date fee received" column says "22/30/2999". oh well, at least the registration is good until 2000/12/31.

Cliff Sojourner, Cisco Systems Inc. cls@cisco.com
(408) 527-7637 170 W. Tasman Drive, SJ CA 95134 bldg H2/cube E2-7

Y2K FTP problem

<amos@nsf.co.il-n0spam>

3 Jan 2000 16:21:40 GMT

Yet another variation: I used an FTP client to download a file, which ended up bearing the date "Dec 10, 1909", even though the file's creation date as listed on the server was "Jan 2, 2000". Checking in debug mode revealed the culprit: a MDTM request returned "191000102072639" which is composed of the now familiar "year 19100"; the FTP client breaks this down to year 1910, month 00 -- which ends up as the last month of 1909.

Amos Shapir, nSOF Parallel Software, Ltd., Givat-Hashlosha
48800, Israel
Tel: +972 3 9388551 Fax: +972 3 9388552

⚡ Y2K funny computer error in Talking Clock

Bruce Stein <bruce42@pacbell.net>
Sun, 02 Jan 2000 23:35:06 -0800

Hi. I use a program to chime the hour and announce the date and time. It is "Talking Clock" version 3.10. and is Copyright 1993 by Aristosoft, Inc. Earlier it announced "Friday, December thirty-first, nineteen ninety-nine". The next day it announced "Saturday, January first, twenty".

Bruce Stein on the Line <bruce42@pacbell.net>

⚡ Y2K compliant? Not possible!

Fred Cohen <fc@all.net>

Mon, 3 Jan 2000 12:45:23 -0800 (PST)

Back in 1984, I wrote a program that ran under System 5 Unix and was tasked with taking care of all things information at a law office. A few years ago, the people who use the system decided to change over to some new commercial software, and I indicated that I would therefore not have to and would not do any Y2K conversion. Come several years later, the 'conversion' to the new system is still running behind the times, and as Y2K looms, I warn the folks who use the system that it is NOT Y2K compliant and that, while most everything should work right through the year 10K and beyond, there was one particular place where I had placed the digits 19 in the code to deal with the fact that the date function (at that time) didn't have a 4-digit mode. After a third warning and assurances that this system was NOT Y2K compliant, they assured me that they would be converted in time.

Come this morning, lo and behold, they are not quite fully converted yet, and are still running my system of 15+ years ago, but surprise of surprises, my system is still doing the right thing as far as they can tell, but the replacement system has destroyed itself. Now I told them again this morning that my system is not Y2K compliant and that they should watch for anything that comes out 19 instead of 20 and manually change it until the new system works, but for the life of me, I cannot figure out how it is still working, given that 19 is hardcoded into it.

Ah well, I guess this Y2K thing was just overblown. Even things that aren't supposed to work seem to be working.

Fred Cohen at Sandia National Laboratories 1-925-294-2087

Fred Cohen & Associates: <http://all.net> - fc@all.net - tel/fax:1-925-454-0171

Fred Cohen - Practitioner in Residence - The University of New Haven

⚡ Re: time left until Y2K ([RISKS-20.72](#))

Daniel Norton <Daniel@DanielNorton.net>

Sun, 02 Jan 2000 21:55:05 -0500

> Time left to January 1 2000:

> -1 years, 11 months, 29 days, 14 hours, 21 minutes, 45 seconds

They've obviously applied the Y2K fix since your post. It now reads:

-1901 years, 11 months, 29 days, 2 hours, 6 minutes, 5 seconds

Daniel Norton

⚡ Re: time left until Y2K ([RISKS-20.72](#))

Matthew Byng-Maddick <mbm@colondot.net>

Sun, 2 Jan 2000 23:44:06 +0000 (GMT)

Interesting to me that most of the bugs seem to be occurring in the systems

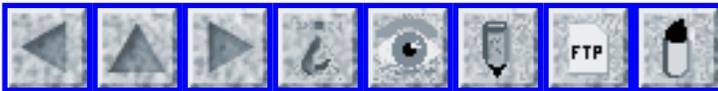
that were supposed to countdown to 12 midnight 1/i/'00. A lot of these

systems are, of course buggy in design, in that they will have

no use after
a certain date, and are therefore buggy from conception through
to
implementation.

Also the other interesting thing about most of the reported
bugs, the
localtime() feature, is that the Camel Book (2nd Edition) is
very clear
about how you should use the year component, ie. not just
"19".(localtime())[5]. Just my 2p worth on this.

Matthew Byng-Maddick mbm@colondot.net <http://colondot.net/>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 74

Sunday 9 January 2000

Contents

- [Y2K multiple billings](#)
[PGN](#)
- [100 years overdue](#)
[PGN](#)
- [Sprint PCS network problems on 1 Jan 2000](#)
[Chenxi Wang](#)
- [MKS Toolkit Y2K glitch](#)
[Ray McCormack](#)
- [Y2K archives](#)
[Lindsay Marshall](#)
[Keith Rhodes](#)
- [Pete de Jaeger bit by Y2K](#)
[Debora Weber-Wulff](#)
- [Northwest Airlines may have leaked credit-card numbers](#)
[Jeremy Epstein](#)
- [Risks of assuming a friendly radio environment](#)
[Fernando C Pereira](#)
- [Re: Just found my first Y2K bug!](#)
[Dana Carpender](#)
- [NTSB website has Y2K test data mixed in with real data](#)

[John Clarke](#)

- [Bogus message in live service for Quicken](#)
[Stephen Page](#)
 - [Re: Microsoft MSIE Y2K Insanity: The last word?](#)
[Andrew D. Fernandes](#)
 - [Teenage computer vandal sentenced to year in jail](#)
[NewsScan](#)
 - [What has changed](#)
[Bertrand Meyer](#)
 - [Network Associates WebShield -- Mail Content Alert](#)
[N/A](#)
 - [SSH: an ineffectual "feel-good" security measure](#)
[William Colburn](#)
 - [Jail for possessing a debugger? More on DVD encryption cracked](#)
[Hamie Marson](#)
 - [CFP: Workshop on Security and Privacy in E-Commerce](#)
[Anup K. Ghosh](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Y2K multiple billings

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

Sat, 8 Jan 2000 12:20:13 PST

The approximately 100,000 merchants using CyberCash's IC Verify transaction software were given the opportunity to install a free upgrade for Y2K, but some of the merchants apparently did not get the fixes. Those who did not do so are apparently rebilling each customer transaction in the new year once each day until the fix is installed. Visa and Mastercard have installed software that attempts to catch the multiple transactions, but you'd better check your statements anyway.

⚡ 100 years overdue

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

Fri, 7 Jan 2000 16:43:45 PST

In one of many reports of off-by-one-hundred Y2K effects, a few dozen

Florida truckers received bills saying they were 100 years late in payments.

Some people received bills for 100 years' back interest. There were even

reports of people whose bank accounts temporarily showed 100 years'

accumulated interest. No surprises there to long-time RISKS readers.

Asymmetrically, we have also had a few reports of people being credited with

100 years worth of interest, although these seem rather specious if you are

getting interest from 1900 to 1999, rather than from 1999 to 1900.

⚡ Sprint PCS network problems on January 1st

Chenxi Wang <cw2e@cs.virginia.edu>

Fri, 7 Jan 2000 17:41:35 -0500 (EST)

I spent the new year in Manhattan and yes, I was in Times Square new year's

eve. After the ball dropped, I started calling friends to wish them a happy

new year, and I was not able to make a single call on my Sprint PCS phone

despite the very strong PCS signal I got. What made it worse was

I could not receive any calls or voice mail during the day on the 1st and my outgoing calls (including calls to check voice mail) were switched to digital roaming calls despite the fact that Manhattan was in Sprint's service area. The problem lasted all day on the 1st, and into parts of the morning on the 2nd.

A later conversation with a Sprint's service representative revealed that Sprint's network was jammed in several metropolitan areas including New York city during the 1st, and they were routing some of their traffic through Bell Atlantic or AT&T's network, which explained the mysterious roaming calls.

Chenxi

MKS Toolkit Y2K glitch

Ray McCormack <raymccormack@home.com>
Sun, 02 Jan 2000 09:34:40 +0000

MKS Toolkit Scheduler (Version 6.1) seems to have a problem with the Y2K date rollover. The application runs fine and must work off the system clock which also appears to be fine. The "Next Event" status however, shows that the next backup is on June 9, 2005 even though it performs daily backups properly.

Ray McCormack, Solutions Consultant, McCormack Consulting
13215-C8 SE Mill Plain blvd. PMB 242 Vancouver, WA 98684 1-360-241-3092

⚡ Y2K archives

<Lindsay.Marshall@newcastle.ac.uk>

Wed, 5 Jan 2000 11:31:35 +0000 (GMT)

I'm sure you'll know about this, but just in case:

<http://y2kmistakes.com>

has a wonderful archive of screenshots of Y2K affected sites.

<http://catless.ncl.ac.uk/Lindsay>

⚡ Y2K archives

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

Wed, 05 Jan 2000 09:03:42 -0500

Some amusing, generally harmless, Y2K snafus can be seen at the following URL.

Look under "affected sites" in the upper left-hand corner.

<http://kwikware.com/y2kmistakes/>

⚡ Pete de Jaeger bit by Y2K

Debora Weber-Wulff <weberwu@tfh-berlin.de>

Thu, 6 Jan 2000 10:43:23 +0100

Sorry, I can't help this:

On <http://www.year2000.com/y2kbugbytes.html>

We have the following headline on Jan. 6, 2000:

Year 2000 Bug Bytes

Updated January 5, 1900 at 23:21 (UTC)

Pete de Jaeger has a nice article on "Why no Chaos?" at <http://www.year2000.com/y2kchaos.html>, however.

Prof. Dr. Debora Weber-Wulff, Technische Fachhochschule Berlin
13353 Berlin, Germany weberwu@tfh-berlin.de <http://www.tfh-berlin.de/~weberwu/>

✈ Northwest Airlines may have leaked credit-card numbers

Jeremy Epstein <jepstein@monumental.com>

Fri, 7 Jan 2000 16:26:03 -0500 (EST)

I saw the following AP item on InfoBeat, a clipping service, but have not yet located it anywhere else. In particular, I have not located this information on NorthWest's web page.

Northwest Airlines is alerting customers who recently made purchases on its Frequent Flier Web site that their credit-card numbers and personal information were unprotected because of a programming glitch. The problem arose when a computer programmer doing maintenance on the site put the system back on line, but forgot to restore the security system. [PGN-ed]

Users have come to expect encrypted traffic, and frequently don't check the icon. Guess we need to be more careful!

⚡ Risks of assuming a friendly radio environment

Fernando C Pereira <pereira@research.att.com>

Fri, 07 Jan 2000 21:53:01 -0500

According to a BBC News story dated Jan 6, 2000

<http://news.bbc.co.uk/hi/english/sci/tech/newsid_592000/592972.stm>, pirate

broadcasters have learned how to use the Radio Data System (RDS) to force

car radios that implement the standard to stay tuned to the pirates'

broadcasts while within range of their transmitters. A radio with RDS active

will switch temporarily to any station that broadcasts the appropriate

embedded digital signal. This is intended to allow reception of brief

traffic announcements, but the pirates repeatedly send the signal in their

broadcasts to keep such radios tuned to them. The problem can be avoided by

switching off the RDS feature on a radio, but then of course one loses

legitimate traffic information.

I only have the slightest acquaintance with RDS so I cannot evaluate the

accuracy of the story, but the RDS standards document "SPB 490 Universal

Encoder Communication Protocol (UECP)" obtainable from

<<http://http://www.rds.org.uk/rds98/mainpublications.htm>> does not mention

security at all.

Fernando Pereira

[Also noted by Aydin Edguer and Russ E. Cage. PGN]

⚡ Re: Just found my first Y2K bug!

Dana Carpender <dcarpend@kiva.net>

Wed, 05 Jan 2000 17:31:04 -0500

Newsgroups: alt.fan.cecil-adams

[Forwarded to RISKS by msb@vex.net (Mark Brader)]

radio2@bigfoot.commm wrote:

> I was just in my friendly neighborhood health food store. Got
> into a brief
> discussion with the guy behind the counter, about Y2K. He
> pointed out a
> box of Barbara's Cereal, which carried an expiration date of
> July 1900!
> Guess it's been sitting on the shelf, there at Flanagan's, for
> a mighty
> long time ...
> -- Geno

I win. Ages ago I realized that my driver's license says it
expired in 1000.

Boy, what's the penalty for driving on a millennium-overdue
license?

Dana W. Carpender <http://www.holdthetoast.com>

Author, How I Gave Up My Low Fat Diet -- And Lost Forty Pounds!

[In case you wondered, YES, it showed 1000 as a 4-digit year.
She lives in Indiana. MSB]

⚡ NTSB website has Y2K test data mixed in with real data

"John Clarke" <jclarke@nortelnetworks.com>

Tue, 4 Jan 2000 11:05:42 -0600

The National Transportation Safety Board maintains a database of all aviation incidents in the US, and provides web access to capsule descriptions of various accidents. These are available by month (<http://www.nts.gov/aviation/months.htm>), so I suspected that there might be some issues with the display or breakdown of the data once we rolled into 2000. The website seems to be working correctly, however, with the exception of a strange entry in January 2000. The accident location (normally City,State) shows "TESTVILLE" and the link is <http://www.nts.gov/aviation/DCA/99A999.htm> (note the 99A999.htm is normally an incident number). The link itself fails to be retrieved, so I assume the test data has been removed from part of the database.

I'm sure we'll see many similar manifestations of Y2K testing in the coming weeks and months.

John Clarke

P.S. Apologies to the citizens of TESTVILLE if it really does exist and a plane crashed there this month.

⚡ Bogus message in live service for Quicken

Stephen Page <mcaa87@dial.pipex.com>

Sun, 02 Jan 2000 19:26:16 +0000

Intuit, who make Quicken (a popular personal and small business financial management application) provide an online service to update share prices, currency rates etc.

Recently users connecting to Intuit's UK server have been automatically offered an application upgrade with the following message:

```
"There is an upgrade available to updated [sic] your current
version of
Quicken 2000.  Would you like to download the update now ? Don't
be afraid,
it is just a test : My name is Nour".  Clicking on "Tell me
more" gives the
message "This version has some improvements in all the area
[sic]".
```

This raises two issues:

1. Either test code has leaked into live service or their site has been hacked. In either case, it is a serious security breach for software which is trusted (e.g., a Trojan horse could create access to users' personal financial data).
2. Intuit has a policy of sell-cheap / charge-lots-for-support which means that there is no way to find out what has happened without waiting for the New Year holiday period to be over, then paying \$1/minute. How nice: the opportunity to pay to get information about their operational failures :-)

This is a major breach of trust and it is to be hoped that Intuit will take it seriously. Perhaps a public apology via RISKS?

⚡ Re: Microsoft MSIE Y2K Insanity: The last word?

"Andrew D. Fernandes" <andrew@cryptonym.com>

Wed, 05 Jan 2000 15:11:36 -0500

I guess I'd only say that if a web developer wanted to use dates in JavaScript, they would:

- 1) have to do a lot of nit-picky detective work, reading documentation from Netscape, Microsoft, and the EMCA, to discover the "correct" way to display the year,
- 2) end up with a script that still wouldn't work on most people's browsers, and,
- 3) learn that they shouldn't have bothered anyway, since some standards group will no doubt later change the "standard" yet again in a way that breaks all previously written scripts.

Yeesh. All this pain, sweat, and confusion just to display a bloody date on a bloody web browser. Small wonder that software reliability issues are gaining attention in the new century...

Andrew D. Fernandes <<mailto:andrew@cryptonym.com>>, Cryptonym Corporation
<<http://www.cryptonym.com>> Telephone +1 919 469 4714

🔥 Teenage computer vandal sentenced to year in jail

"NewsScan" <newsscan@newsscan.com>
Wed, 22 Dec 1999 07:31:37 -0700

Described by his lawyer as "a disturbed young man" suffering from depression, 19-year-old Jay Satiro of New Rochelle, NY, has been

sentenced
to one year in jail for cracking into America Online computers
and causing
an estimated \$50,000 in damages. Satiro had been an AOL
technical support
volunteer and had used knowledge obtained from his job to break
into the
company's systems and replace AOL programs with his own. [AP/
USA Today,
21 Dec 1999) <http://www.usatoday.com/life/cyber/tech/ctg955.htm>;
NewsScan Daily, 22 Dec 1999, reproduced with permission]

⚡ What has changed

<Bertrand_Meyer@eiffel.com>

Thu, 30 Dec 99 13:57:45 PST

Call me naive, but I can't help marvel, risks or not, at what is
going on.
Here I am, on the penultimate day of the millennium (OK, I know,
that will
be next year, but what's wrong with celebrating twice?),
listening through
minuscule speakers on my computer to a broadcast of perfect
sound quality
from a site half-way around the world. It's playing something I
know, but I
can't just recall what it is. So I catch four Italian words on
the fly and
type "senza perdere un momento", not forgetting the quotes, into
AltaVista.
A second later, and perhaps fifteen seconds after I first asked
myself the
question "what is this?", I have the answer, thanks to someone
at Stanford
who keeps the full text of Donizetti's "Don Pasquale" on his Web
pages.

Just a few years ago none of this would have been possible. I

wouldn't have had a clue where to begin my search. Even a trip to the UCSB library would have been unlikely to help.

The prospects of using computers for advancement of human knowledge are all around us; they are staggering. Let's remember this as we continue (as well we should) worrying about the associated risks.

Bertrand Meyer, Interactive Software Engineering/Monash University

<http://eiffel.com>, <http://tools-conferences.com>

⚡ Network Associates WebShield -- Mail Content Alert

<[irrelevant]>

Tue Jan 04 04:17:31 2000

Network Associates WebShield SMTP V4.5 Beta 2 on prometheus2 intercepted a mail from <owner-risks@csl.sri.com> which caused the Content Filter HTTP to be triggered.

[Lots of RISKS issues lately have been blocked. Perhaps Y2K is now considered to be a dirty word. In some other cases RISKS copies were rejected because they were too long. Apparently some temporary Y2K virus filters believe that if mail is longer than 10K, it might contain a virus or Trojan horse. The assumption that viruses are bigger than 10K seems specious. PGN]

🔥 SSH: an ineffectual "feel-good" security measure

"Schlake (William Colburn)" <schlake@nmt.edu>

Mon, 20 Dec 1999 00:34:14 -0700

When I first read the report of RST breaking the netscape algorithm I was caught up in the moment. Netscape should have known better than do something so foolish! Then I read the next comp.risks and I felt like a fool. There is a great risk in pretending to have security when you really have none.

I think many people believe that ssh protects them from wrongdoers, and that nothing bad can happen to them if they use ssh. The authors of the Internet Auditing Project(1) have a good story to tell about ssh, as do the people who run the web site for rootshell.org(2). Some sysadmins here at work are rabid about ssh. They have disabled telnet and rlogin for "security" reasons, and naively believe that ssh is somehow more secure.

Ssh protects the data stream between two secure machines. Anyone sitting between the two machines can't tell what is going on in the ssh stream because of the encryption. The risk to the user is assuming that either end is secure.

Where I work, the important servers don't run telnet or rlogin, because those protocols are "insecure". The servers only run ssh. Our network is switched. In order to sniff packets an attacker either needs to

be in the machine room with a cable plugged into the switch, or they need to be on either of the two machines that the traffic is going between AND they need to be root. If they are root on either machine, then they can:

- a) read the unencrypted TTY instead of the encrypted stream
- b) read the local secret keys and decode the stream on the fly
- c) replace ssh with a Trojan
- d) trace the program and extract the unencrypted data from the write()s
- e) many more things I can't think of right now

If no one has compromised my system, then it is safe to use telnet to login between machines. If someone has compromised my system however, I might as well use telnet since I can't trust ssh anymore. If no one has compromised my system, and I need to login over an untrusted network, and I have a secure machine to login from, then ssh is the perfect tool.

Where am I going to find a secure machine outside my network? I bet there are lots of secure machines all over the place, but I will never know which ones they are. If security is really important to me, I will never log in to any computer from any other computer I don't own (and hence trust) myself. That means I that if I need to login to work when I am off site, that I need to have my own laptop that I keep powered down, encased in cement, buried in a vault, and guarded by an army (and even then can I really be sure it is secure)?

Last week I spent an entire day at work wondering how to protect my mail server from all the trouble that is expected from people trying to hide

under the veil of Y2K. I took ssh out of the inetd.conf, and told everyone that they have to log in on console from now on.

(1): http://www.securityfocus.com/templates/forum_message.html?forum=2&head=32&id=32

(2): <http://www.rootshell.org/maillinglist-archive/rs-25>

✶ Jail for possessing a debugger? More on DVD encryption cracked (20.66)

Hamie <hmarson@ibm.net>

Fri, 17 Dec 1999 08:29:03 +0000

"Daniel A. Graifer" <dgraifer@cais.com> makes an interesting point that a debugger & a screwdriver may be analogous when comparing intent to commit a crime. But I believe that the menace behind the law & the practice of encrypting region coded disks is far more insidious...

It's not about stopping casual, or even determined piracy. They can encrypt & degrade all they like to try & foil copying. But at the end of the day, a picture has to appear on a screen somewhere for someone to see it. There is no way they can stop a determined person or corporation from taking a copy of that unless they own & control everything in between.

Their attempt to push this law through is more akin to denying you access to a screwdriver to fix your own lock in case it breaks, or because you don't like the colour of the door... Why shouldn't I have the means to play a legally bought DVD on my laptop using Linux? Why should I have

to pay money
(If it were possible) to some faceless company who may perhaps
come out with
a DVD player, that may create a player for my favourite OS, on
my favourite
hardware?

✦ CFP: Workshop on Security and Privacy in E-Commerce

"Anup K. Ghosh" <anup.ghosh@computer.org>

Wed, 5 Jan 2000 09:26:56 -0500

The First Workshop on Security and Privacy in E-Commerce
Athens, Greece, 4 Nov 2000 <http://www.rstcorp.com/conferences/wspeg00/>

held in conjunction with the ACM Conference on Computer and
Communications
Security, <http://www.ccs2000.org>

Preliminary Call for Papers

The First Workshop on Security and Privacy in E-Commerce seeks
to bring
together practitioners and researchers to address the real-world
security
and privacy concerns in e-commerce. We are seeking contributions
on topics
in security and privacy that will enable the e-commerce systems
of tomorrow
to be developed more securely and robustly without compromising
individual
privacy rights. The workshop will focus on group discussion and
collaboration in identifying the important problems and
potential solutions
in this important topic area. Proceedings from the workshop
will be
published and distributed to attendees. Highest quality papers
will be

published in a book and widely distributed after the workshop.
We are seeking research papers, business case studies, or system designs that address security and privacy concerns in any of the following topic non-exclusive areas:

- anonymizing e-commerce/Web transactions
- component-based software in e-commerce
- databases access control
- denial of service attacks and countermeasures
- detecting anomalous database transactions
- detection and recovery from Internet-based attacks
- e-commerce protocols
- e-commerce systems
- Internet client risks
- malicious software or Trojan functionality
- mobile agents in e-commerce
- novel attacks and countermeasures
- privacy negotiation/bartering
- privacy risks with cookies/tokens/identifiers
- software analysis and certification.

Submissions will be accepted for regular research papers, case studies, and panel proposals. Abstract submission deadline: May 1, 2000.

See <http://www.rstcorp.com/conferences/wspeg00/> for complete Call for Papers.

Anup K. Ghosh, Ph.D., Program Chair



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 75

Sunday 16 January 2000

Contents

- [More on Pentagon satellite data outage](#)
[PGN](#)
- [Credit-card data used for extortion](#)
[Steven M. Bellovin](#)
- [British Visa source-code compromised](#)
[Frank Markus](#)
- [Greek tax information system experiences black-out](#)
[Diomidis Spinellis](#)
- [Berlin Fire Department with Y2K Problem?](#)
[Debora Weber-Wulff](#)
- [Kremlin press office Y2K problems](#)
[Greg Lastowka via Declan McCullagh](#)
- [Re: Y2K99?????](#)
[Drew Davis via Mark Brader](#)
- [Sidekick98 Y2K bug squashed](#)
[Michael Froomkin](#)
- [Lookout Outlook!](#)
[Bruce Sterling](#)
- [Resume system creates "Profile" for you... without permission](#)
[Tom Malaher](#)

• [Woman ordered to pay back four pence](#)

[Alan Barclay](#)

• [More on RISKS-20.73](#)

[Clive D.W. Feather](#)

• [Info on RISKS \(comp.risks\)](#)

✂ **More on Pentagon satellite data outage ([RISKS-20.72](#))**

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

Sat, 15 Jan 2000 22:21:16 PST

We noted in [RISKS-20.72](#) that the Pentagon satellite intelligence system was unable to process data for 2.5 hours after the midnight GMT Y2K rollover.

Apparently the situation was much worse than initially realized. UPI

reported on 12 Jan 2000 that the problem was actually self-inflicted,

resulting from a misguided supposedly preventive software patch in a

sensitive NRO intelligence program called Talent Keyhole at Fort Belvoir.

For the next few days, there was only a trickle of data from 5 satellites.

✂ **Credit-card data used for extortion**

"Steven M. Bellovin" <smb@research.att.com>

Mon, 10 Jan 2000 14:31:29 -0500

The New York Times today reported an extortion attempt involving credit

card numbers stolen from online merchant CD Universe. Someone who called

himself "Maxim" and claimed to be Russian said that he had

copied 300,000 credit card numbers from their system, and that he would post them on the Internet unless he was paid \$100,000. The article quoted the chairman of eUniverse, the company that operates the site, as confirming that Maxim did indeed have their data. eUniverse declined to pay the \$100,000; Maxim posted 25,000 card numbers to a Web site. Several thousand people downloaded the file before it was yanked.

What's interesting, though, is not that this can occur. In fact, security folks have been warning for years about wholesale theft of card numbers. But most sites can't or won't do anything about it. Consider, for example, the security statement currently posted on the cduniverse.com Web site (I saw no mention of the incident):

Security - Is Internet Shopping Safe?

We have all heard a lot of talk about whether shopping on the internet is safe. The main concern of online shoppers is that their credit card information will somehow end up in the wrong hands. We use Netscape's Secure Commerce Server technology, which encrypts your order information, keeping it private and protected. It's a Netscape technology called "SSL" (Secure Sockets Layer) and it's used by us and all the other major commercial shopping sites, including: The Wall Street Journal, Barnes & Noble Books, FTD Flowers, Microsoft, and Netscape itself. It is actually safer to transmit your credit card info over the Internet than it is to

use your credit card around town.

By focusing on transport encryption, they miss the point entirely. The real risk is bulk theft, as has happened here. Consider the following text from their Web site:

If you have previously placed an order and want to use the same credit card, you can select the "Use previous credit card info" option. You do not need to enter your credit card information unless your credit card expiration date has passed.

By maintaining this information online, they (and many other Web merchants, of course) are inviting trouble.

It is tempting to say "use SET", which would provide for digitally-signed payment authorization. Unfortunately, SET may send your credit card number to the merchant anyway. Many stores use credit card numbers as the database key for user purchasing patterns; they didn't want to lose the link if SET ever took off. But this means that card-number data still exists on the merchant's site somewhere.

The CD Universe security statement concludes with this note:

What most people don't realize is that shopping with your credit card is actually safer than paying by check. In the event that there is a problem with your purchase, the credit card company will remove the purchase from your bill and the on-line merchant is not paid. In the event that your credit card number is stolen, the credit card companies do not

hold you

responsible for any unauthorized purchases.

It is, I believe, accurate, though there may still be \$50 liability to the consumer under U.S. law. (And they don't say anything about credit card numbers belonging to non-Americans, even though they list shipping charges for international destinations.) But *someone* is going to have to swallow the fraudulent charges -- and we won't see an overall improvement in computer security until the *real* injured parties apply appropriate pressure.

[The NYT article also noted by Scott Lucero. PGN]

🔥 British Visa source-code compromised

"Frank Markus" <fmarkus@pipeline.com>

Sun, 16 Jan 2000 09:44:26 -0500

According to an article by Jon Ungoed-Thomas and Stan Arnaud in the *Sunday Times* of London for 16 Jan 2000, British hackers have compromised the source code for the Visa card system and have sought ransom for it.

Excerpts from the story which I found online under the headline ``Hacker gang blackmails firms with stolen files'' follow:

Visa confirmed last week that it had received a ransom demand last month,

believed to have been for 10M pounds. "We were hacked into in mid-July

last year" [despite layers of firewalls], said Russ Yarrow, a company

spokesman. It is understood the hackers stole critical source code, and

threatened to crash the entire system. Visa's system handles nearly 1

trillion pounds of business a year from customers holding 800M Visa cards.

No further incursions were detected. [PGN-ed]

But this begs the question of what they should have done -- if anything --

after receiving notification that their system had been penetrated. After

CD Universe's credit-card database was compromised by a hacker/blackmailer,

their system was (apparently) shut down temporarily and its customers

notified (of which I, alas, was one.) Visa seems to have had no fall back

plan for this crisis except to call in the police and hope for the best. If

the hackers have not disseminated the code more widely, Visa has been very

lucky and the damage has been controlled. But how certain can anyone be of

that? And how certain can they be that there was only one penetration?

⚡ Greek tax information system experiences black-out

Diomidis Spinellis <dspin@aegean.gr>

Fri, 14 Jan 2000 13:04:38 +0300

According to the Athens financial newspaper "Naftemporiki" (14 Jan 2000,

p. 7) the Greek tax information system TAXIS has been down since Tuesday

January 11th. All computerised regional state finance offices (DOY) have

been affected as they are unable to connect to the system's main

computer.

I was personally able to verify this at my local state finance office where tax liability certificates were not issued on Wednesday. According to Naftemporiki, the affected services include the provision of tax liability certificates, the issue of new tax registry numbers (AFM), and the validation of ledgers and receipts. Many of these services are needed for the lawful conduct of business.

According to sources within the ministry (department) of finance, the system's hard disk was overloaded by the large number of applications that were running on it. Another source claims that while data was transferred from one hard disk to a larger one an error resulted in the loss of all data. The disk (referred to in the article as "the system's main memory") has been sent to the United Kingdom to be repaired and to attempt to recover the lost data.

Some of the above accounts are contradictory: it is not clear whether the disk suffered a catastrophic failure, or the problem is a result of a human error. In any case, the reported attempt to recover data from the disk in question suggests that database resiliency, backup and recovery procedures, and contingency planning were not adequate. In addition, it appears that a system whose failure can disrupt business, trade, and everyday life of millions of citizens (tax liability certificates are needed for many important transactions) was not designed to withstand centralised failures.

Diomidis Spinellis, University of the Aegean
<http://kerkis.math.aegean.gr/~dspin>

✶ Berlin Fire Department with Y2K Problem?

Debora Weber-Wulff <weberwu@tfh-berlin.de>

Wed, 12 Jan 2000 12:04:39 +0100

There has been heated debate in the Berlin newspapers about the fire department's computer problems over New Year's. It seems that just after midnight the dispatching systems broke, but they broke in an unexpected way: they told the dispatchers that an alarm had been given to a fire station, when in reality the fire station did not receive the alarm, and kept playing cards and wondering why there were no fires this nice New Year's Eve. [This is in itself a very hard to avoid security risk.] At one point an exasperated police car drove to a fire station, which was just around the corner to ask if they needed an engraved invitation or what?!

The systems also logged fire engines as being somewhere in use when they were actually sitting in the fire house, and thus tried to alarm fire engines that were further away from the fire.

There has been lots of finger-pointing. The systems were "Y2K-secure" because they were tested for this 2 weeks ago. [Gosh, I didn't realize that someone had found out how to prove by test that software functions properly!
-dww] The chief fire fighter had to be called in at about 1.30

am to figure
out what to do, eventually falling back on very old equipment:
people, paper
and pencil.

The blame has been put on the massive number of calls to the
fire department
during the night, which had overloaded the system. Maybe I ought
to invest
in a second fire extinguisher...

Some on-line articles:

[http://www.BerlinOnline.de/wissen/berliner_zeitung/
archiv/2000/0103/lokales/0064/index.html](http://www.BerlinOnline.de/wissen/berliner_zeitung/archiv/2000/0103/lokales/0064/index.html)

<http://www.tagesspiegel.de/archiv/2000/01/04/ak-be-kr-13983.html>

<http://www.tagesspiegel.de/archiv/2000/01/06/ak-be-st-24269.html>

Interesting too the article in August 1999

<http://www.tagesspiegel.de/archiv/1999/08/05/ak-be-st-23279.html>

where an official says that the fire department is just
spreading panic by
saying that they will be having problems on New Year's Eve...

Prof. Dr. Debora Weber-Wulff, Technische Fachhochschule Berlin
weberwu@tfh-berlin.de, <http://www.tfh-berlin.de/~weberwu/>

⚡ Kremlin press office Y2K problems (via Declan McCullagh)

Greg Lastowka <greglas@yahoo.com>

Fri, 14 Jan 2000 06:28:09 -0800 (PST)

The Kremlin press office's computer communication system was
victimized by
Y2K, blocking their ability to send e-mail. Reportedly, they
will have the
problem fixed by ``the end of the month''. [Source: Agence
France Presse,
13 Jan 2000]

Greg Lastowka, University of Virginia Law School
lastowka@virginia.edu
<http://hobbes.itc.virginia.edu/~fgl2q/home.html>

✉ Re: Y2K99?????

<Drew Davis via Mark Brader>
Fri, 14 Jan 2000 23:07:02 GMT

Newsgroups: alt.fan.cecil-adams

"Wulfdog" <johnw@icok.net> excerpt:

>I turned on a 286 PC in my office today. I looked at the date
>and it said
>Jan 05 2000. Previously I had ran the date forward on my new
>HP and it went
>to 2099 and rolled back to 1980. I quickly ran the 286 date up
>and to my
>surprise it went to 2099 and rolled back to 1980. I wonder
>what those
>little diskettes with the Y2K test were actually checking for,
>the size of
>your wallet/checking account? My other question is. Will any
>of us
>remember to tell the New Millennium babies that they are the
>ones who will
>see the "REAL Y2K bug"?

Hey, I've got a Y2K issue. My fax driver/app "Delrina WinFax
Lite 3.0 Fax
Administrator" can't recognize years 00 to 09 as the send
date. I have to
go and change the send date to 99 or before. Neat.

-Drew

⚡ Sidekick98 Y2K bug squashed

"Michael Froomkin - U.Miami School of Law" <froomkin@law.miami.edu>

Tue, 11 Jan 2000 11:51:03 -0500 (EST)

Having assured everyone that Sidekick98 was Y2K OK, Starfish software's calendar/scheduler product developed a bug last week in which attempts to view your daily appointments produced a complaint of "Invalid file to complete this action! mast:wk". Some users also reported troubles with past "to-do" items not done failing to appear on the current day's list.

Starfish have released <A HREF = "<ftp://ftp.starfish.com/pub/sk98/sk98patch.exe>">a patch that certainly fixes the first problem and may fix the second too (I didn't have it so I cannot report on this).

Although there is a Sidekick99, many users refuse to "upgrade" because the feature set in '99 is a feeble subset of the more powerful '98.

No word from the company on what was missing from their testing procedure.

A. Michael Froomkin, U. Miami School of Law, P.O. Box 248087,
Coral Gables,
FL 33124 USA +1 (305) 284-4285 <http://www.law.tm>
froomkin@law.tm

⚡ Lookout Outlook!

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

Sat, 15 Jan 2000 18:13:09 PST

>From: Bruce Sterling <bruces@well.com>
>Subject: Viridian Note 00124: Viridian Movement Officially

Viridian Curia Member Laura Stinson points out that people unwise enough to use "Microsoft Outlook" cannot read the entire "Manifesto of January 3, 2000." That's because one line of the text happens to begin with the word "begin," followed by two spaces. When Microsoft Outlook sees this, it interprets everything that follows as an attachment.

I'll bet you didn't know that you could blind Microsoft Outlook readers merely by placing the innocuous term "begin" in a text, thus giving a preferential advantage to readers who spurn Microsoft products. Now you know this. I hope you don't put your newfound powers to any sinister use.

🔥 Resume system creates "Profile" for you... without permission

Tom Malaher <risks@netstart.com>
Thu, 13 Jan 2000 17:07:57 -0700

I got the following e-mail out of the blue today:

> We have added your resume to our Resume Database. We have received your
> resume in response to an ad; or your resume was available in the resume
> database of an employment site to which we subscribe.

[...description of Metro Information Services elided...]

> If you are interested in a position with Metro, please use the

following

> URL to verify/update your e-Profile on Metro's Resume Database. The URL
> below will connect you to a private area of Metro's website containing
> only your information. The information you provide us is not publicly
> available on the Internet. Metro does not sell, trade, or publicly
> distribute any personal information we receive from any source.

> When updating your e-Profile, do not click the <Submit> button until after
> you have completed updating your resume information. Once the <Submit>
> button is clicked, you will no longer have access to your e-Profile.
> After you have submitted changes to your e-Profile, if your expertise
> matches an open position, a recruiter may contact you about the
> opportunity.

>
> <http://metroweb.MetroIs.com/eProfile/<string of random digits>>.asp

So they've created a "secret" web page for me, from which I can "update" my profile. Presumably as soon as I <Submit> the profile, this secret file will go away.

Risks? Here are some I can think of:

- 1) They did this without asking me. It appears that they slurped a resume I have posted on my web site. (And didn't do a very good job of it, much of the information is missing or incorrect.)
- 2) There's no authentication on the URL. Whoever receives or is able to snoop the "secret" URL is able to update my profile, at which point I will not be able to! What if my e-mail address has

changed

since I created the web page?

3) How do I go about *keeping* my profile up to date with them, since

this "secret" URL goes away after the first submission?

Presumably

there is some mechanism, and maybe they would e-mail that to me as

well, once I've completed the initial update... it just gets worse...

Tom Malaher - Web Developer - NetStart Consulting Ltd. - www.netstart.com

⚡ Woman ordered to pay back four pence

Alan Barclay <gorilla@elaine.drink.com>

Tue, 11 Jan 2000 11:07:43 -0500

http://news.bbc.co.uk/hi/english/uk/scotland/newsid_598000/598625.stm

The BBC is reporting of the problems Mrs Pringle George is having after receiving benefits in June & July last year, after being injured in a car accident. In November, she was contacted by the Credit Recovery Group of the Benefits Agency, who informed her that she was accidentally overpaid for one week of benefit Pounds 43.16, however when she wrote a cheque to repay the overpayment, the cheque was for the amount 43.12, an underpayment of 4 pence.

Mrs George said she was shocked when she received a letter at the weekend informing her of the debt and telling her that legal action was

being
considered.

A spokesman for the Benefits Agency said he was unable to discuss individual cases but explained that if the agency received a cheque for the wrong amount the computer automatically produced a generalised letter. "The computer cannot differentiate between 4p and 400 pounds," he said.

Two questions come to mind, first why was there a five month gap between the overpayment and the first attempt to reclaim payment, and secondly why can't the computer differentiate? It would seem simple to write off small amounts, and indeed most billings systems do this.

More on [RISKS-20.73](#)

"Clive D.W. Feather" <clive@demon.net>
Mon, 10 Jan 2000 08:32:11 +0000

All following up to 20.73:

(1) Robert Rathbone <rr@dragonheart.net> writes:
> It would be like performing a check to see if there were more
> than 60
> seconds in a minute.

There can be 61 seconds in a minute. It's called a "leap second".

(2) Andrew M Greene <agreene@pageflexinc.com> talks about *The New York Times* changing its numbering. Does this mean that numbers are going to be

duplicated for the next year or two, or will all references to issues since 1898 be suddenly invalid ?

(3) "John J. Francini" <francini@progress.com> writes:
> The UNIX98 standard changed the localtime() function so that the year
> value is redefined to be the "year in the current century"

This is the second time I've seen this claim recently. As far as I know it is false, since such a change would be incompatible with existing practice and also with the ISO C Standard. Can someone provide a URL for the UNIX98 definition?

Clive D.W. Feather <clive@demon.net> +44 20 8371 1138
Internet Expert, Demon Internet <http://www.davros.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 20: Issue 76

Sunday 23 January 2000

Contents

- [The Net enables a Farther Confessor Website](#)
[PGN](#)
- [U.S. National Archives loses 43K e-mail messages](#)
[Jeremy Epstein](#)
- [Rhode Island computer arrested innocents](#)
[David Mediavilla Ezquibela](#)
[Mark Richards](#)
- [Hackers steal passwords, cause havoc](#)
[NewsScan](#)
- [Bug lists babies as aged 100](#)
[Brian Randell](#)
- [Y2K and satellite orbit predictor software](#)
[Erling Kristiansen](#)
- [Y2K Problems with Flight Sim 2000 Professional Edition?](#)
[David H Smith](#)
- [U.S. removes most restrictions on encryption software](#)
[NewsScan](#)
- [Re: British Visa source-code compromised](#)
[G Bell](#)
- [Re: Woman ordered to pay back four pence](#)

[G Bell](#)

● [Re: Lookout Outlook!](#)

[Dan Franklin](#)

[Laura Stinson](#)

● [Here's an update to the simulated Kangaroos story](#)

[Walter and Paul Mallory via Paul Green](#)

● [Computers, Freedom & Privacy 2000 Advance Program](#)

[PGN](#)

● [2000 IEEE Symposium on Security and Privacy](#)

[PGN](#)

● [Info on RISKS \(comp.risks\)](#)

✶ The Net enables a Farther Confessor Website

"Peter G. Neumann" <Neumann@CSL.sri.com>

Fri, 21 Jan 2000 07:23:17 -0800 (PST)

There are plenty of opportunities for sin on the Internet, but precious few sources of absolution. So today, Britain's only Christian radio station launches an online "confession box" for sinful surfers who feel the need to repent. The website, www.theconfessor.co.uk allows users to file their wrongdoings - in return for a comforting Bible text. The automated response will not reflect the gravity of the offence: coveting thy neighbour's wife and throttling thy neighbour's tearaway teenage son elicit similarly sympathetic passages. They see a series of contemplative texts and then a page offering the chance to type out a confession. They are reassured with the message: "All you type remains on your computer and will not be transmitted in any way to anyone else. This is between you and God and your

privacy is respected." [Source: *The Guardian* online, 21 Jan 2000]

✶ U.S. National Archives loses 43K e-mail messages

Jeremy Epstein <jepstein@monumental.com>
Tue, 18 Jan 2000 15:32:11 -0500 (EST)

The Washington Post, 6 Jan 2000, reported that the National Archives lost an estimated 43,000 e-mail messages (the number is a guess based on the number of users). The backup system also failed: the contractor was not doing as instructed (according to the Archives). The audit log, which might have shed light, had been turned off because it reduced performance.

The Assistant Archivist says that they've improved the backup system now, but "the safest way to save important messages is to print them out".
Hurrah for the paperless office!

RISKS: What good are backups & audits if they're not used correctly?

Full article at
<http://www.washingtonpost.com/wp-srv/WPlate/2000-01/06/1241-010600-idx.html>

✶ Rhode Island computer arrested innocents

<David Mediavilla Ezquibela>
Thu, 20 Jan 2000 01:45:48 -0800 (PST)

According to Noticias Intercom (in Spanish)

<http://www.noticias.com/noticias/2000/0001/n0001202.htm>

quoting *Providence Journal*, the Rhode Island police have stopped arresting people, because they found that their new system Justice Link asked them to arrest eight innocent people. Justice Link is made by Oracle and Systems & Computer Technology Corp. Developers found 350 bugs to trigger detention.

✶ Rhode Island computer arrested innocents

"Richards, Mark" <MarkR@ifpcorp.com>

Thu, 20 Jan 2000 17:47:32 -0500

[...]

The risk is that the innocent victim argues with the police and ends up dead ... or worse, is beaten, thrown before a judge and falsely convicted.

Makes the prospect of encountering criminals a safer bet than a drive through Rhode Island.

The part of this that really gets my ire: "We knew we had bad data in the old warrant system," Harrall said. He added that neither Oracle nor SCT are at fault, instead attributing a large part of the problem to a rush to get the system up and running to meet a Y2K deadline. "I will not hang those on the vendor," Harrall said.

Thanks for hanging it on the innocent public, instead.

⚡ Hackers steal passwords, cause havoc

"NewsScan" <newsscan@newsscan.com>

Wed, 12 Jan 2000 10:15:58 -0700

A 16-year-old hacker, one of a group calling themselves Global Hell, infiltrated Pacific Bell's Internet service and lifted codes to the accounts of 200,000 subscribers. When Eldorado, Calif., detectives checked his bedroom last week, they found that he'd decrypted 63,000 of those accounts, causing PacBell to advise those subscribers to change their passwords. Authorities found the boy after he broke into the computers of an Eldorado Hills Internet service provider and began bragging about his exploits in a chat room. According to a sheriff's detective, the same teenager hacked into 26 other sites, including a master computing system at Harvard, before he was arrested Dec. 14. Authorities expect to charge him with unlawful computer access and grand theft next month. [Source: *Los Angeles Times*, 12 Jan 2000, <http://www.latimes.com/business/20000112/t000003535.html>;

NewsScan Daily, 12 Jan 2000]

⚡ Bug lists babies as aged 100

Brian Randell <Brian.Randell@newcastle.ac.uk>

Mon, 17 Jan 2000 15:11:39 +0000

Thousands of newborn babies have been listed officially as 100 years old.

Computers at English register offices are refusing to recognise the year as

2000 and are printing 1900 on birth certificates. [...]

[Source: The (London) *Times*, 17 Jan 2000; The full story is online at:

<http://www.the-times.co.uk/news/pages/Times/frontpage.html?1069542>]

Brian Randell, University of Newcastle, Newcastle upon Tyne, NE1 7RU, UK

+44 191 222 7923 <http://www.cs.ncl.ac.uk/~brian.randell/>

⚡ Y2K and satellite orbit predictor software

Erling Kristiansen <erling@wm.estec.esa.nl>

Mon, 17 Jan 2000 16:18:31 +0100

A popular free-of-charge predictor for UNIX platforms, SatTrack V3.1,

went completely haywire.

On 7 Jan. it told me:

Date: XXX -358Jan01 (I think the XXX should be the day of the week)

UTC : -358-11:-32:-94

Countdown to next pass: 657443 days 11 hours 32 minutes 10 seconds

(this is rather precisely 1800 years)

Satellite position: 0.0 deg lat. 0.0 deg. long. (does not move)

In all fairness, this version is a few years old; the latest version

comes at a cost, and is said to be Y2K compliant.

Another popular program, WinOrbit 3.5 for Windows 95/98 nearly got it right.

I found only one problem:

If you want to print the prediction for several future passes, you get a

pop-up on which you have to enter the starting time for the calculation.

There is a "NOW" button that fills in this entry, giving the year as 00.

00 means 1900 to the program.

You can type 2000 instead of 00, and you get the correct results.

Easy, once you know. But it took some time to first discover that the

results were wrong, then figure out the work-around.

I am told that yet another predictor works fine in 2000, as long as you use

the orbit parameters, the so-called "2-line elements", from end 1999, but

goes wrong with parameters that have a year entry of 00. I haven't got the details.

Erling Kristiansen

✶ Y2K Problems with Flight Sim 2000 Professional Edition?

David H Smith <david.h.smith@gecm.com>

Mon, 17 Jan 2000 10:58:36 +0000

I managed to get Microsoft Flight Sim 2000 Pro Edition for Xmas, great!

After installing I went to the Microsoft web site and found an update - of

course there was one - 9 megabytes in total. I downloaded it, installed it,

everything was fine.

A few days later I did my in-frequent disk cleanups, etc. I had not run

scandisk for ages so set it off. I was surprised when it

announced that it had found a bad file. The file was with one of the Flight Sim 2000 files, and the problem was that it had an invalid date. This problem occurred with all the Flight Sim 2000 files that had come as part of the update I had downloaded.

Was it a Y2K problem? I'm not sure. Everything worked okay and McAfee Virus Checker didn't complain about funny dates on the files. Of course, it could have been a problem with the disk scan program.

Dave Smith

🚀 U.S. removes most restrictions on encryption software

"NewsScan" <newsscan@newsscan.com>

Thu, 13 Jan 2000 09:17:28 -0700

Finally relenting to continued pressure from the technology industry, the Clinton Administration has decided to remove virtually all restrictions on the exportation of powerful data encryption software, and to require companies to seek government permission only when they plan to sell the technology to a foreign government or military organization. Companies will still be prohibited from selling to seven nations thought to be supporting terrorism: Iran, Iraq, Libya, Syria, Sudan, North Korea, and Cuba. Industry leaders expect the decision to give a significant boost to the sale of U.S. technology, and Novell chairman Eric Schmidt says it "clearly

sets the stage
for the next big growth phase of the Internet." [AP/*San Jose
Mercury News*,
13 Jan 2000 <http://www.sjmercury.com/svtech/news/breaking/merc/docs/009455.htm>;
NewsScan Daily, 13 Jan 2000]

[Open-source software is apparently unrestricted. PGN]

⚡ Re: British Visa source-code compromised ([RISKS-20.75](#))

<BELLG@mimi.com.au>
Tue, 18 Jan 2000 10:37:57 +1000

Before we all get too carried away about perceived risks, a few questions need to be asked. In the interests of credibility, we should not fall into scaremongering.

As supposedly expert practitioners in computing related risks, we should be sure we have established a logical thread before we reach conclusion. Otherwise we *risk* being classified with the boy who cried wolf, and thereby exclude ourselves from contributing to improved security and risk management.

In the Visa case, what source code was *stolen*? It is extremely unlikely that it was *the source code for the Visa card system* as stated! There is no such thing. Like any system, it would consist of many source libraries, each relating to different modules of the overall system. So we should be asking what source was copied? (You can hardly say it was *stolen*, as that

would imply that it was taken away, leaving the rightful owner without possession of the item of stolen property, and we all know that is not what happens in such cases. In a shop like Visa, the code promotion system maintains multiple copies in the migration libraries, so erasure of the sole copy is highly unlikely)

Was it the card number validation module? Perhaps part of staff payroll processing? or Some CGI for their public web site? or Perhaps an in-house written reporting tool? Was it the current version, an old one, a pre-production one, a half-tested development one?

As it appears that Visa is not stating what code was copied, it is rather hard to support the assertion that their system was *compromised* in the manner implied. And what is the basis for stating that *Visa seems to have had no fall back plan*. What fallback is appropriate when source is illicitly copied? What is the threat we need to counter?

It all depends on what was copied.

⚡ Re: Woman ordered to pay back four pence ([RISKS-20.75](#))

<BELLG@mmi.com.au>

Tue, 18 Jan 2000 10:37:57 +1000

Not all billing systems write off *small debts*, or at least didn't always do so. When I left UK in 1981 after living and working there for a time, I

took with me my Barclay Visa card and used it for expenses as I took the long route home to Australia via the US. Naturally, it took a few months for all my purchase charges to catch up with me. (1981 was before widespread on-line merchant transaction processing). Finally all the charges were in and I paid out my statement by wire transfer from my Australian bank. Of course I left it to the last minute to pay, and the payment got to my Visa account a day or so late.

So, next month I received a statement with one line item - Credit Charges: 40pence (equiv \$US.050), contained in an envelope bearing 85 pence in postage. At \$A5 (\$US3.00) in fees per wire transfer, I chose to ignore the statement. Next month, another statement for 40p. And then another. And then nothing. I presume I appeared on the delinquent debtors list for recovery action and someone at Barclays then realised they had spent PndsStg2.55 in postage while attempting to recover 40p from the other side of the world!

Although I've been back to UK numerous times since (twice in the employ of a Bank and carrying a Corporate Visa card), I do wonder what Barclay's reaction would be if I ever applied for another card with them? Am I black listed as a credit risk forever? Or maybe their system has been revamped a few times since then and the delinquents list wasn't transferred across?

🔥 Re: Lookout Outlook! ([RISKS 20.75](#))

Dan Franklin <dan@dan-franklin.com>

Mon, 17 Jan 2000 11:15:02 -0500

> Viridian Curia Member Laura Stinson points out that people
unwise enough
> to use "Microsoft Outlook" cannot read the entire "Manifesto
of January 3,
> 2000." That's because one line of the text happens to begin
with the word
> "begin," followed by two spaces. When Microsoft Outlook sees
this, it
> interprets everything that follows as an attachment.

I tried this at work as soon as I heard about it. Of 5 Outlook
users
reporting back, 4 were indeed "blinded" - they did not see the
line
beginning "begin" or any text thereafter. One of them reported
seeing an
attachment she could not open.

One user saw the whole test text with no problem. He believes
that the
difference is that he gets his mail from a Microsoft Exchange
server rather
than directly (using IMAP? I don't use Outlook so I don't know
what the
other choices are).

So unfortunately, rather than giving a preferential advantage to
those who
"spurn Microsoft products" as the original message suggests,
this problem
may be taken as evidence that if you buy one Microsoft product,
then (to
coin a phrase) you "gotta get them all!"

Dan Franklin, Comverse Network Systems

🔥 Re: Lookout Outlook! ([RISKS 20.75](#))

"Laura Stinson" <lstinson@empathy.com>

Wed, 19 Jan 2000 21:34:29 -0700

[Many of you wrote that you were unable to reproduce this problem.

This item is in response to a message to Linda from Tom Neff... PGN]

I found it running Outlook 98 on NT. Another person reports reproducing the problem on Outlook Express 5 on NT, but NOT on Outlook Express 5 on NT, Outlook 97 on NT, or Outlook Express 4.5 on MacOS. I don't know of any reason why OS version (NT vs. 95/98/00) would make a difference, but who knows what evil lurks in the relevant DLLs? Since neither Bruce nor Microsoft are paying me to debug, I'm disinclined to investigate further.
[...]

Laura Stinson <lstinson@empathy.com>

🔥 FW: Here's an update to the simulated Kangaroos story ([RISKS-20.47](#))

"Green, Paul" <Paul_Green@stratus.com>

Fri, 17 Dec 1999 11:42:47 -0500

[Many of you have sent in the Kangaroo story that was excerpted from

rec.humor.funny in [RISKS-20.47](#). This item from Paul Mallory was

forwarded to RISKS by Paul Green. PGN]

> Date sent: Thu, 16 Dec 1999 15:49:34 +0000 (GMT)
> From: walter.mallory@gecm.com (Walter Mallory)
> Subject: (Fwd) Re: Probably should be in .

software_eng,

> To: mallory@west.net
> Organization: GEC Marconi Dynamics, Inc.

>

> Adrian Frith wrote:

> This sounds like an urban legend and when I first heard of it
(as reported
> on the Defence Systems Daily web site). I thought that it was
until I

> read the correction story shortly afterward. I have attached
the

> correction below. It is even weirder than the original.

> What those Killer Kangaroos really fired, 29 November 1999

> On Friday DSD told the story of the killer kangaroos. Now we
know the

> truth. And it is even weirder: the kangaroos threw beach balls!

> Dr Anne-Marie Grisogono, Head, Simulation Land Operations
Division at the

> Australian DSTO has told us what actually happened and we are
delighted to

> set the record straight.

> "I related this story as part of a talk on Simulation for
Defence, at the

> Australian Science Festival on May 6th in Canberra. The Armed
> Reconnaissance Helicopter mission simulators built by the
Synthetic

> Environments Research Facility in Land Operations Division of
DSTO, do

> indeed fly in a fairly high fidelity environment which is a
4000 sq km

> piece of real outback Australia around Katherine, built from
elevation

> data, overlaid with aerial photographs and with 2.5 million

realistic 3d

> trees placed in the terrain in those areas where the
photographs indicated
> real trees actually exist.

> "For a bit of extra fun (and not for any strategic reason like
kangaroos

> betraying your cover!) our programmers decided to put in a bit
of animated

> wildlife. Since ModSAF is our simulation tool, these were
modeled on

> ModSAF's Stinger detachments so that the associated detection
model could

> be used to determine when a helo approached, and the behaviour
invoked by

> such contact was set to 'retreat'. Replace the visual model of
the Stinger

> detachment in your stealth viewer with a visual model of a
kangaroo (or

> buffalo...) and you have wildlife that moves away when
approached. It is

> true that the first time this was tried in the lab, we
discovered that we

> had forgotten to remove the weapons and the 'fire' behaviour.

> "It is NOT true that this happened in front of a bunch of
visitors

> (American or any other flavour). We don't normally try things
for the

> first time in front of an audience! What I didn't relate in
the talk is

> that since we were not at that stage interested in weapons, we
had not set

> any weapon or projectile types, so what the kangaroos fired at
us was in

> fact the default object for the simulation, which happened to
be large

> multicoloured beachballs.

> "I usually conclude the story by reassuring the audience that
we have now

> disarmed the kangaroos and it is again safe to fly in
Australia."

> Andy

✦ Computers, Freedom & Privacy 2000 Advance Program

<neumann@csl.sri.com>

Sun, 9 Jan 2000 15:58:11 -0800 (PST)

The Tenth Conference on Computers, Freedom and Privacy (CFP2000)
April 4-7, 2000, Westin Harbour Castle, Toronto, Ontario, Canada

For additional details and registration forms see <http://www.cfp2000.org>

Featured speakers:

- Tim O'Reilly, founder and CEO of O'Reilly & Associates, Inc., open source champion
- Neal Stephenson, author of Cryptonomicon, Snow Crash, The Diamond Age, and Zodiac: The Eco Thriller
- Austin Hill, co-founder and president of Zero-Knowledge Systems
- Duncan Campbell, freelance investigative journalist and TV producer, discovered the existence of the ECHELON system
- Jessica Litman, Professor of Law at Wayne State University
- Whitfield Diffie, Distinguished Engineer at Sun Microsystems, co-inventor of public-key cryptography
- Steve Talbott, editor of the "NetFuture - Technology and Human Responsibility" online newsletter

Scholarships are available for students as well as law enforcement officials, prosecutors, and criminal defense attorneys. Scholarships cover conference registration, travel, and hotel expenses. Application

deadline: January 31. See <http://www.cfp2000.org/scholarships/>

** TUESDAY, APRIL 4

9 AM - 12:30 PM - Tutorials, Workshop on Freedom and Privacy by Design

- Constitutional Law in Cyberspace
- How Did We Get Where We Are: A Brief History of Privacy and Surveillance in the U.S.
- Intellectual Property

2 - 5:30 PM - Tutorials, Workshop on Freedom and Privacy by Design

- The Electronic Communications Privacy Act
- Everything You Need to Know to Argue About Cryptography
- Privacy Policies: Public Protection or Trojan Horse?

8 PM - Welcome Reception

** WEDNESDAY, APRIL 5

8:45-9:30 AM - Opening Session - Keynote speaker: Austin Hill

9:30-10:45 AM - Domain Names Under ICANN: Technical Management or Policy Chokepoint

11:15 AM - 12:30 PM - New Justice Information Technologies: Does Existing Privacy Law Contemplate Their Capabilities?

12:30-2pm - Lunch - Luncheon speaker: Steve Talbott

2:15-3:30 PM - Security and Privacy in Broadband Internet Services

4-5:15 PM - Privacy Commissioners: Powermongers, Pragmatists or Patsies?

5:15-7:15 PM - The 2000 Orwell Awards and Reception

7:30-9:30 PM - Dinner - Dinner Speaker: Neal Stephenson

9:30 PM - midnight - BOFS

** THURSDAY, APRIL 6

8:45-9:30 AM - Keynote speaker: Duncan Campbell

9:30-10:45 AM - Intellectual Property and the Digital Economy

11:15 AM - 12:30 PM - CFP2000 Hot Topics - TBA

12:30-2pm - Lunch - Luncheon speaker: Jessica Litman

2:15-3:30 PM - Parallel Sessions

- Free Expression v. Privacy
- Infomediaries and Negotiated Privacy
- Human Subjects Research in Cyberspace
- Network Society as Seen by Two European Underdogs
- The Media and Privacy

4-5:15 PM - "Who Am I and Who Says So?": Privacy and Consumer Issues in Authentication

5:15-6 PM - Keynote Speaker: Tim O'Reilly

7:00 - EFF Pioneer Awards Reception

9:30 PM - midnight - BOFS

** FRIDAY, APRIL 7

8:45-9:30 AM - Keynote speaker: TBA

9:30-10:45 AM - Internet Voting: Spurring or Corrupting Democracy

11:15 AM - 12:30 PM - Negotiating the Global Rating and Filtering System: Views of the Bertelsmann Foundation's Self-regulation of Internet Content Proposal

12:30-2pm - Lunch - Luncheon speaker: Whitfield Diffie

2:15-3:30 PM - Parallel Sessions

- Broadband and Speech
- Is Technology Neutral? Space, Time and the Biases of Communication
- Governance of the Internet
- Personal Data Privacy in the Pacific Rim
- Campaign Finance Law and Free Expression

4-5:15 PM - 10 Years of CFP: Looking Back, Looking Forward

✦ 2000 IEEE Symposium on Security and Privacy

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

Sat, 22 Jan 2000 11:54:26 PST

May 14-17, 2000, The Claremont Resort, Oakland, California

Sponsored by the IEEE Technical Committee on Security and Privacy
In cooperation with the International Association of Cryptologic
Research

Jonathan Millen, General Chair; Li Gong, Vice Chair
Michael Reiter, Program Co-Chair; Roger Needham, Program Co-Chair

PRELIMINARY PROGRAM (Subject to Change) [Abridged for RISKS]

** Monday, 15 May 2000

9:00-10:30 Access Control I

Access Control Meets Public Key Infrastructure,
Or: Assigning Roles to Strangers
Amir Herzberg, Joris Mihaeli, Yosi Mass, Dalit Naor,
Yiftach Ravid (IBM, Israel)

A Security Infrastructure for Distributed Java Applications
Dirk Balfanz (Princeton University, USA) and Drew Dean (Xerox
PARC, USA)

A Practically Implementable and Tractable Delegation Logic
Ninghui Li, Benjamin Grosf (IBM T.J. Watson Research Center,
USA), Joan Feigenbaum (AT&T Research, USA)

11:00-12:00 Applications of Cryptography

Practical Techniques for Searches on Encrypted Data
Dawn Song, David Wagner, Adrian Perrig (University of
California, Berkeley, USA)

Efficient Authentication and Signature of Multicast Streams
over Lossy Channels

Adrian Perrig, Dawn Song, Doug Tygar (University of California,
Berkeley, USA), Ran Canetti (IBM T.J. Watson Research Center,
USA)

1:30- 3:00 Panel: Is privacy too costly to implement?

Moderator: Cynthia Irvine, Tim Levin

3:30- 5:00 Protocol Analysis and Design

Searching for a Solution: Engineering Tradeoffs and the
Evolution of Provably Secure Protocols

John A Clark, Jeremy L Jacob (University of York, UK)

Authentication Tests

Joshua D. Guttman, F. Javier Thayer (MITRE, USA)

Protocol-Independent Secrecy

Jonathan Millen, Harald Ruess (SRI International, USA)

** Tuesday, 16 May 2000

9:00-10:30 Panel: Does open source really improve system
security?

Moderator: Lee Badger

11:00-12:00 Intrusion Detection

Using Conservation of Flow As a Security Mechanism in Network
Protocols

John R. Hughes, Tuomas Aura, Matt Bishop (University of
California, Davis, USA)

Logic Induction of Valid Behavior Specifications for Intrusion
Detection

Calvin Ko (NAI Labs)

1:30- 3:00 Assurance

Using Model Checking to Analyze Network Vulnerabilities

Ronald W. Ritchey (Booz Allen & Hamilton, USA), Paul Ammann

(George Mason University, USA)

Verifying the EROS Confinement Mechanism

Jonathan S. Shapiro, Samuel Weber (IBM T.J. Watson Research Center)

Fang: A Firewall Analysis Engine

Alain Mayer, Avishai Wool, Elisha Ziskind (Bell Labs, Lucent, USA)

3:30- 5:00 5-minute presentations on developing research

[Contact reiter@research.bell-labs.com to propose a 5-minute talk.]

** Wednesday, 17 May 2000

9:00-10:30 Key Management

A More Efficient Use of Delta-CRLs

David A. Cooper (National Institute of Standards and Technology, USA)

An Efficient, Dynamic and Trust Preserving Public Key Infrastructure

Albert Levi, M. Ufuk Caglayan (Oregon State University, USA)

Kronos: A Scalable Group Re-keying approach for Secure Multicast

Sanjeev Setia, Samir Koussih, Sushil Jajodia, Eric Harder (George Mason University, USA)

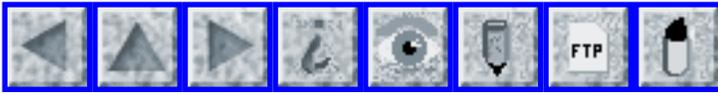
11:00-12:00 Access Control II

LOMAC: Low Water-Mark Integrity Protection for COTS Environments

Timothy Fraser (NAI Labs)

IRM Enforcement of Java Stack Inspection

Ulfar Erlingsson, Fred B. Schneider (Cornell University, 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 20: Issue 77

Saturday 29 January 2000

Contents

- [Report on identity theft](#)
[Mich Kabay](#)
- [Japanese Government Websites hacked](#)
[Ole J. Jacobsen](#)
- [Japanese department-store credit-card fraud](#)
[Chiaki Ishikawa](#)
- [Superbowl XXXIV Web-filtered: adult porn?](#)
[John Wharton](#)
- [Porn spammers getting cute](#)
[Jim Griffith](#)
- [Lessons of Y2K](#)
[Toby Gottfried](#)
- [Parisian programmer makes his own smartcard](#)
[NewsScan](#)
- [DVD lawyers make "trade secret" public](#)
[Declan McCullagh](#)
- [French spies listen in to British business phone calls](#)
[Declan McCullagh](#)
- [DoE password policy comic relief?](#)
[Mike Williams](#)

- [Re: U.S. removes most restrictions on encryption software](#)
[Kevin Mitchell](#)
 - [Simson Garfinkel's *Database Nation*](#)
[Peter G. Neumann](#)
 - [REVIEW: "Hackers: Crime in the Digital Sublime", Paul A. Taylor](#)
[Rob Slade](#)
 - [REVIEW: "Implementing IPsec", Elizabeth Kaufman/Andrew Newman](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Report on identity theft

Mich Kabay <mkabay@compuserve.com>

Wed, 26 Jan 2000 09:27:21 -0500

Caitlin Liu of the *Los Angeles Times* published a thorough report on identity theft on 16 Jan 2000 (front page). In one case, 22-year-old San Diego college student Jessica Smith had her car stolen with her handbag inside. Although the car and bag were recovered, someone stole her identity. She nearly got fired from her new job when a background check showed that "she" had outstanding warrants for prostitution. She was unable to obtain credit, phone service or even to rent an apartment. With the help of a sympathetic police investigator, Smith was able to prove her innocence of the charges a reversal of the usual burden under criminal law, where usually the state has to prove guilt. She obtained judicial documents explaining that her identity had been stolen; nevertheless, she has been hauled into police stations to be fingerprinted to prove that she is indeed

the person authorized to carry those documents.

Image Data LLC, an identity-fraud prevention service based in Nashua, NH, commissioned a study in September 1999 that suggested that one out of five Americans or a member of their family have been victimized by identity fraud. [Readers should always be wary of statistics that report how many "members of your family" or "people you know" have particular characteristics: it is possible that a single person can be reported by multiple people. The over-counting bias increases as a function of sample size and of social relationships among the sample population.]

🔥 Japanese Government Websites hacked

"Ole J. Jacobsen" <ole@cisco.com>
Wed, 26 Jan 2000 07:14:39 -0800 (PST)

Japan called an emergency meeting Wednesday to boost computer security after humiliating raids on government Websites by hackers, who linked one to a pornographic site and attacked Japan's war record on another. The announcement came amid revelations that the site at the Science and Technology Agency had been penetrated twice in two days, and that key data on another site, including census information, had been erased.

[Source: http://dailynews.yahoo.com/h/nm/20000126/wr/japan_hackers_4.html,

Japan Calls Emergency Meeting As Hackers Hit Again, By Elaine Lies,

Reuters, 26 Jan 2000; via Dave Farber's IP list]

🔥 Japanese department-store credit-card fraud

Chiaki Ishikawa <Chiaki.Ishikawa@personal-media.co.jp>

Wed, 26 Jan 2000 21:08:13 +0900 (JST)

It is widely reported in the Japanese media that the credit cards issued by a large department store chain, Takashimaya, were target for fraud.

It seems that some of these cards were duplicated by a third party and innocent owners were charged for shopping they never did on their own, etc..

The incidents of such mis-use has multiplied since last October and the Takashimaya store finally has decided to issue whole new set of the credit cards, about 0.3 million cards in total. They were mailed to the card owners this month and they are supposed to be move over to the new cards by the end of this month.

The articles I read mention that some dubious figures were spotted last year who were seemingly looking at the cards held by the customer waiting in line at the cashier or cards laid face up while the store clerk was doing necessary paperwork for the purchase, etc.. The very typical case of shoulder-surfing. However, the spotted figures didn't have a good memory obviously and were seen to hitting their hand-held telephone keypads or similar devices!

BTW, it always amazes me that Japan is just a few years behind

the USA in terms of these fraud and abuses in terms of credit cards/e-commerce business and not many people in Japan seem to be paying attention to what goes on in USA. I was quite taken aback to read that the people (store clerks presumably?) spotted such dubious figures and did nothing at all. The newspaper articles quoted the store management as saying just looking at other people's cards are not a just cause for arrest or anything drastic. Surely.

(This lax attitude is quite different from a case where someone at the department store checking counter was passing the customer credit card through another reader. One customer asked the clerk questions and was not satisfied with the answers and fetched the store security person and put the clerk into the custody of the police or whoever on the spot. This was reported earlier in RISKS if I am not mistaken. Surely, in that case, the clerk was operating as a bad guy, but that the store management didn't do a thing about this case in Japan until this month (issuing new cards) is a little bit disappointing. Japanese consumer laws are not well developed and I am afraid that some of the customers whose cards were mis-used had to negotiate the damage recovery with the department store. There is no 50 dollars limit like that if I recall correctly in Japan! This hurts.)

After reading the articles and looking at the new design of the cards, it occurred to me that the card issuers might well consider making the numbers

DIFFICULT TO READ by means of ungainly color combination (or no color at all in a patterned background, etc.). After all, the card reader reads the numbers from the magnetic stripe and the legitimate card owners can read the numbers at leisure if they want to make mail order purchases, etc.. This would make the reading difficult for the shoulder-surfing artists.

In the articles, it was also noted that the credit cards issued by a same organization have a tendency to have similar string of digits (near the beginning?) and thus easy to copy by the shoulder surfers. This could again possibly be made more difficult by truly randomizing the issued numbers using MD5 or whatever at the cost of administration.

Just a thought.

Chiaki Ishikawa, Shinagawa, Tokyo, Japan 142-0051

⚡ Superbowl XXXIV Web-filtered: adult porn?

John Wharton <jwharton@netcom.com>

Wed, 26 Jan 2000 14:22:56 -0800 (PST)

Just heard a report on CBS network radio that net-savvy football fans around the country are being stymied in their efforts to learn about this Sunday's Superbowl. Seems the Web-filtering software installed on browsers, e.g., in certain public libraries spots the "XXX" in "Superbowl XXXIV" and interprets this to mean it's an adult porn site. John Wharton
[via Dave Farber's IP list]

✶ Porn spammers getting cute

Jim Griffith <griffith@netcom.com>

Tue, 25 Jan 2000 21:06:11 -0800 (PST)

I just got nailed by a porn spammer getting clever. The spammer in question sent me e-mail stating that I'd been sent a cyberspace greeting at www.hypergreeting.com (a legitimate e-card site). However, while the text description of the link says "www.hypergreeting.com", the actual link behind the text led to a hardcore site. I'm just glad I didn't decide to check it out at work.

[We've had several cases like this in RISKS. PGN]

✶ Lessons of Y2K

"Toby Gottfried" <toby6700@earthlink.net>

Sun, 23 Jan 2000 20:26:49 -0800

Amidst all the hoopla over Y2K, we have much to contemplate. There is a big lesson to learn from it about our dependency on technology. For all the advances in capability we have made (including those that make possible the distribution of these words), we have created systemic risks.

Under evolution organisms adapt (slowly!) to their environment. Technology represents the opposite approach: humans attempting to adapt

their

environment to themselves, in their current state. Each step of "technolution" solves or eases some existing problem, but may change the overall landscape. In the last couple of centuries, the pace has accelerated, and luxuries became conveniences became necessities.

Our senses developed to a good level of acuity over the millenia, now they are often necessarily aided by external devices. Our brains have large, unused capacities, but we rely on easily lost electronic notepads instead of our memories. Cars take us from one place to another through suburbs spread beyond walkable distances, fouling the air along the way. Many people have trouble walking any distance at all (which problem can be made worse by having to carry a heavy external "brain", which can also be lost or stolen). Essential knowledge is placed on a worldwide network, which must work all the time. Food comes from all over the world, as does the energy to move us and our goods, and change the temperature of our surroundings (intentionally or otherwise). Now human reproduction is becoming more technological. It is a very complex system which we take for granted.

The very minor problem of Y2K was sufficiently widespread to threaten to disrupt much or all of this. But Y2K was relatively easy to anticipate and head off. Something else might not be. Recent news stories have appeared about the President proposing defenses against cyber-terrorism and a lowered redundancy and reliability in the deregulated national power grid. The survivalists now have to figure out what to do with their provisions, but

every-man-for-himself is not the right way to back up this system.

Do we have the vision to reap the benefits of technology and avoid the pitfalls or will we change our environment beyond our ability to adapt to it fast enough ? As the now ancient margarine commercial reminded us, "It's not nice to fool Mother Nature".

🔥 Parisian programmer makes his own smartcard

"NewsScan" <newsscan@newsscan.com>
Wed, 26 Jan 2000 09:00:30 -0700

A resourceful French computer programmer has been arrested on counterfeiting and fraud charges after he purchased 10 Paris Metro tickets using his homemade smartcard. After proving the smartcard worked, Serge Humpich then tried to sell his "invention" to the Cartes Bancaires consortium, an amalgamation of 176 smartcard-issuing banks, for about \$1.5 million. Humpich faces a seven-year jail term, but insists that he never intended to steal; rather, he was tricked into purchasing the Metro tickets after Carte Bancaires officials insisted he demonstrate the card worked. Meanwhile, Humpich's lawyer says Humpich deserves compensation for the four years of work it took him to crack the 640-bit encryption key used to verify the "digital signature" on the cards. "It is an invention," he said, noting that Humpich had patented his discovery before contacting the Cartes Bancaire

group. Humpich's card is designed to respond positively no matter what PIN number is typed in. [MSNBC, 25 Jan 2000, <http://www.msnbc.com/news/361936.asp> via NewsScan Daily, 26 Jan 2000]

⚡ DVD lawyers make "trade secret" public

Declan McCullagh <declan@well.com>
Wed, 26 Jan 2000 15:11:44 -0800

Lawyers representing the DVD industry got caught in an embarrassing gaffe when they filed a lawsuit [against a Norwegian teenager and his father] and accidentally publicized the computer code they wanted to keep secret. The DVD Copy Control Association included its "trade secret" source code in court documents, but forgot to ask the judge to seal them from public scrutiny. Whoops.

In a hastily arranged hearing Wednesday morning, DVD CCA lawyers asked Santa Clara Superior Court Judge William J. Elfving to correct their oversight, and he agreed to keep the document confidential.

It may be a little late. The document is dated 13 Jan 2000 and is widely available on the Web. The owner of one site that placed the 140KB declaration on-line says over 21,000 people have downloaded it so far. [...]

[DVD Lawyers Make Secret Public, Declan McCullagh <declan@wired.com>, see <http://www.wired.com/news/politics/0,1283,33922,00.html>

Distributed via Declan's POLITECH, a moderated mailing list of politics and technology. See <http://www.well.com/~declan/politech/>]

✦ French spies listen in to British business phone calls

Declan McCullagh <declan@well.com>

Wed, 26 Jan 2000 15:37:53 -0800

French intelligence is intercepting British businessmen's calls after investing millions in satellite technology for its listening stations. The French government upgraded signals intelligence last year. Now secret service elements are using it to tap into commercial secrets. At least eight centres, scattered across France, are being "aimed" at British defence firms, petroleum companies and other commercial targets. Eavesdroppers can "pluck" GSM digital mobile phone signals from the air by targeting individual numbers or sweeping sets of numbers. Targets have included executives at British Aerospace, British Petroleum and British Airways, according to French sources. Senior executives have been told not to discuss sensitive issues on mobile phones, and BAe staff have been told to be "especially careful" during campaigns for new business, such as the current battle to supply Eurofighter missiles. [...]

[Source: French spies listen in to British calls, James Clark, <http://www.sunday-times.co.uk/news/pages/sti/2000/01/23/stinwenws03006.html?999>

Distributed via Declan's POLITECH, a moderated mailing list of

politics

and technology. See <http://www.well.com/~declan/politech/>]

⚡ DoE password policy comic relief?

Mike <John.Michael.Williams@Computer.org>

Wed, 26 Jan 2000 06:48:32 -0500

[The] DOE security "czar" ... said it is now virtually impossible for employees to transfer nuclear secrets from classified to unclassified computer networks ...

To quote Don Adams of "Get Smart" - Would you believe ... no more than once a week? ... once a day?

Many [nuke] employees used their last names or initials, and some simply typed "password" when logging onto classified networks, he said.

Now, [the czar] added, "we have a password policy that I would put up against any in industry and academia."

Password Policy? Reusable passwords to guard nuclear secrets? Doesn't this constitute a well-known RISK, of breach followed by fusion?

Does anybody in the press ever question these publicity handouts? Do we in the industry just sit on our hands, letting this travesty continue?

[Source: Energy Chief Touts Security Upgrades at Nuclear Labs, Vernon Loeb, *The Washington Post*, 26 Jan 2000, A13:
<http://www.washingtonpost.com/wp-srv/WPlate/2000-01/26/1261-012600-idx.html>]

✂ Re: U.S. removes most restrictions on encryption software (NewsScan)

Kev <klmitch@MIT.EDU>

Tue, 25 Jan 2000 17:16:57 -0500

Although the restrictions on encryption software have indeed been revamped, there are still a number of problems with the new regulations, as described at http://www.epic.org/crypto/export_controls/joint_release_1_00.html. In particular, PGN's comment, "Open-source software is apparently unrestricted," does not appear to be entirely true, according to my reading of the material available (Note: IANAL). In particular, you may not post source code directly to citizens of the 7 terrorist nations mentioned in the article. You can, however, place your source code on a publically accessible Web site or ftp site, and you apparently don't have to worry about who actually accesses it (again, IANAL). You must, however, inform BXA about what you intend to do and either send them a copy or tell them the URL. Some people I know are also of the opinion that these regulations would conflict with the GPL.

In short, I feel the new regulations are a step in the right direction, but they unfortunately have not been completely removed, and that's what should eventually happen.

Kevin L. Mitchell <klmitch@mit.edu> <http://web.mit.edu/klmitch/>

[www/](#)

[I may appear to have oversimplified, but if something is posted on

a Website, it would appear to be effectively open to the world! PGN]

🔥 Simson Garfinkel's *Database Nation*

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

Thu, 27 Jan 2000 10:10:59 PST

Simson Garfinkel

Database Nation: The Death of Privacy in the 21st Century
O'Reilly & Associates, Sebastopol CA 95472

The following words of Ralph Nader are on the back cover of this book,

and very appropriately highlight this excellent book:

"Database Nation by Simson Garfinkel is a graphic and blistering

indictment of the burgeoning technologies used by business, government,

and others to invade the self -- yourselves -- and restrict both your

freedom to participate in power and your freedom from abuses of power. The right of privacy is a constitutionally protected right, and

its erosion or destruction undermines democratic society as it generates, in one circumstance after another, a new kind of serfdom.

This book is one that you're entitled to take very personally."

You will find this book very much in tune with what you have been reading in

RISKS and in Lauren Weinstein's PRIVACY FORUM all these years. Simson has

brought it all together very nicely in a highly readable book.

🔥 REVIEW: "Hackers: Crime in the Digital Sublime", Paul A. Taylor

Rob Slade <rslade@sprint.ca>

Wed, 26 Jan 2000 20:17:22 -0800

BKHAKERS.RVW 991024

"Hackers: Crime in the Digital Sublime", Paul A. Taylor, 1999,
0-415-18072-4, U\$24.99

%A Paul A. Taylor drpaul_a_taylor@yahoo.co.uk

%C 11 New Fetter Lane, London, England, EC4P 4EE

%D 1999

%G 0-415-18072-4

%I Routledge

%O U\$24.99 +44-71-842-2214 info@routledge-ny.com

%P 198 p.

%T "Hackers: Crime in the Digital Sublime"

Following in the footsteps of Sarah Ford, Dorothy Denning, and Ray Kaplan, Paul Taylor is attempting to open the world, and world view, of those who make informal attempts to penetrate computer and communications security to the security "expert." The book tries to explain motivations, culture, and background, with a view to the benefits of a dialogue between the official guardians and those who pry at the gaps in the armor. Using extensive interviews with people from both sides of the divide, Taylor attempts to put forward the reality behind the hype.

Chapter one concentrates on the terms; hack, hacker, and hacking; emphasizing the original meaning of creative and useful mastery of the

technology. Hacking culture is reviewed quite thoroughly in chapter two, although perhaps not enough attention is paid to the divisions and continuum that exists. (I was amused by the note in the preface to the effect that nobody would admit to distributing viruses: virus writers still occupy the lowest rung of the hacking ladder.) Motivation is explored, and possibly too much credence given to self-reporting, in chapter three. Chapter four is a marvel, a first rate examination, and indictment, of the state of computer security (or, perhaps, insecurity). Arguments for, and against, dialogue with, and employment of, those who have done unauthorized security breaking are given in chapter five. Chapter six, however, turns to presenting a number of sociological theories about why hackers might be marginalized. This material seems to have no purpose other than to propose that such people are being treated unfairly. Chapter seven is worse: even given the wretched track record of computer ethics literature it is disappointing in that presents little content that is germane to the discussion, and seems to wander off into miscellaneous speculation. The conclusion, in chapter eight, also meanders, but tries to dispel a number of myths that have grown up around the hacker idea.

The book will probably not be a popular hit, which is a pity. I would suggest two reasons for the low profile. The first is that Taylor is making a conscious effort to avoid sensationalism, and, indeed, to counter the sensational, and misinformed, reports of computer security

penetration that are prevalent in the popular media. The second reason is not inherent in the nature of the material and is somewhat unfortunate: Taylor's writing style is more "academic" than is necessary, using, for example, the passive voice most of the time. (I found the use of the word "whilst" to become quite jarring after a few pages.) A good copy editing would help: your humble scribe, world's worst proofreader that he is, still found a number of grammatical errors, even outside of the quotations.

(Oddly, for all its academic formality, endnotes, and bibliography, the work falls short in terms of clarity of references and citations. I am quoted on page 84, but I can't figure out how. I am also dying to know who the other "Dr. Taylor" is.)

The extensive use of interview materials, and quotations from other works, is both a strength and a weakness. No one perspective is allowed to dominate, and a great many arguments and opinions are presented. The constant quotes from a variety of sources, however, often reduce the readability of the work. I found the book very difficult and time consuming to get through. Added to this, Taylor's aversion to contaminating the source material with his own analysis ensures that the text is very demanding of the reader's own analytical skills and work.

Taylor does make a serious effort to give a fair and even presentation to both sides of the argument, but it is still fairly obvious that his

sympathies lie in "detente." The title of the book itself indicates this.

There is a discussion of the derivation and evolution of the "hacker" term, but the acceptance of the "popular" status of the word to mean those who break into computers also allows those who break into computer systems to present arguments for their behaviour as a kind of discovery learning, without the supporting evidence that would otherwise be necessary. In this, Taylor's work shares a weakness with other, similar, books on the topic: "hacker" claims are taken at their own valuation without much analysis of either factual or motivational claims. Taylor has a great deal more material and a wider range of direct contacts than Levy (cf. BKHACKRS.RVW), Sterling (cf. BKHKRCRK.RVW), or Dreyfus (cf. BKNDRGND.RVW) and his conclusions are significantly more reliable, but the fundamental defect remains.

There are also gaps in the coverage. Taylor does not dwell on the basic fragility of data, nor the tendency of digital systems to catastrophic failure under even the most minor perturbation. There are also indirect effects of unauthorized system penetration. To give only one example, the regular choice of NASA as a target, and the media hype over even minor success, has had a negative impact on budget appropriation, and therefore on the space program as a whole. You can't claim much for the advancement of knowledge out of that.

With all the problems presented above, I still highly recommend

this

work to anyone in the security field, or to anyone who wants to understand either security work or an important part of the computer culture. For all its flaws, Taylor's book is the most extensive and detailed examination of the cracker phenomenon I have ever read. He exposes a number of nasty little secrets that the computer industry as a whole would prefer to forget. Hopefully this work will be continued, expanded, and refined, to become a valuable classic in technical security literature.

copyright Robert M. Slade, 1999 BKHAKERS.RVW 991024
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

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

⚡ REVIEW: "Implementing IPsec", Elizabeth Kaufman/Andrew Newman

Rob Slade <rslade@sprint.ca>
Thu, 27 Jan 2000 07:15:43 -0800

BKIMPIPS.RVW 991029

"Implementing IPsec", Elizabeth Kaufman/Andrew Newman, 1999,
0-471-34467-2, U\$49.99

%A Elizabeth Kaufman

%A Andrew Newman

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 1999

%G 0-471-34467-2

%I John Wiley & Sons, Inc.

%O U\$49.99 416-236-4433 fax: 416-236-4448 rlangloi@wiley.com

%P 271 p.

%T "Implementing IPsec: Making Security Work on VPNs,

Intranets, and Extranets"

This book starts with a rough, and even aggressive, manner. It continues the same way. But what makes for a rather abrasive introduction also makes for a very practical and solid guide to designing, evaluating, and thinking about network security.

Chapter one is brief, really only an overview of the structure of the book.

Part one actually starts in the next chapter, and looks at what you need to

know going in. Chapter two looks at the basic information you need before

you even start to consider security, and provides a highly practical guide

to documenting the network. (Oh, sure, you *all* have fully documented

networks. No, thank you, I don't want to buy any bridges.) Security

should, of course, start with a policy, but chapter three outlines a

real-world approach when you don't have one. The law is an underappreciated

factor in implementing security, and a highly instructive run through of

related aspects is presented in chapter four.

Part two reviews the essentials of the technology. Chapter five covers the

Internet Protocol, and the security weaknesses built into what it does.

Cryptography cannot be covered in a single chapter, but I was a bit

surprised that there is not even a discussion of relative strengths in the

basics that are explained in chapter six. Keys and key management are

discussed reasonably well in chapter seven.

Part three looks at implementation considerations. Chapter eight gives an extremely helpful, if somewhat depressing, look at possible problems and inherent conflicts. Chapter nine offers some useful pointers, but is more about the generic types of implementations.

Part four gets down to the brass tacks of buying. Chapter ten gives some rough pointers on how to evaluate vendors. But the really useful stuff is in chapter eleven, which provides the details, with explanations, for an entire RFP.

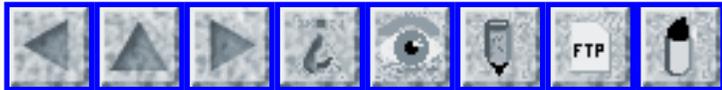
RFC 2401 is printed as an appendix.

The authors are not out to produce a fun read, but they have a very nice sense of sarcasm--and know when to use it. Subtle digs pop up in the text frequently, and are generally right on target. The humour included in the work is germane to the topic, and helps to highlight and render memorable important basic concepts.

As the authors are at pains to point out, IPsec is by no means a mature technology. Security practitioners, and network managers, are fortunate to have such a guide to avoiding the worst mistakes as they take the first steps into a new area.

copyright Robert M. Slade, 1999 BKIMPIPS.RVW 991029
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

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



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 78

Sunday 6 February 2000

Contents

- [CIA Director Deutch and MLS](#)
[Jeremy Epstein](#)
- [CERT Advisory CA-2000-02](#)
[CERT Advisory](#)
- [NSA system inoperative for four days](#)
[PGN](#)
- [Leak lets 64 get rich quick](#)
[David Shaw](#)
- [EFIS failure main suspect in Crossair crash](#)
[Peter B. Ladkin](#)
- [Terra spacecraft problems](#)
[Peter B. Ladkin](#)
- [Patients will be able to wear their hearts on the Internet](#)
[NewsScan](#)
- [Yahoo suit compares cookies to stalking](#)
[NewsScan](#)
- [China to require encryption information](#)
[NewsScan](#)
- [Study criticizes health sites for privacy intrusions](#)
[NewsScan](#)

- [AT&T Business Internet Service DNS major outage 28 Jan 2000](#)
[Randy Holcomb](#)
 - [More risks with MS Outlook](#)
[Jason Axley](#)
 - [Who is at risk with this virus advertisement?](#)
[Bob Heuman](#)
 - [Organisms do not adapt to their environment!](#)
[Bob Frankston](#)
 - [*Fatal Words*](#)
[Bob Frankston](#)
 - [abcnews.com manually updates copyright year](#)
[David Glicksberg](#)
 - [People For Internet Responsibility issues and status report](#)
[Lauren Weinstein](#)
 - [New Security Paradigms Workshop 2000: Call For Papers](#)
[Crispin Cowan](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ CIA Director Deutch and MLS

Jeremy Epstein <jepstein@monumental.com>
Tue, 1 Feb 2000 09:40:14 -0500 (EST)

An article in **The New York Times** 1 Feb 2000 details former CIA Director Deutch's use of unclassified Macintosh computers in his homes to store thousands of highly classified documents on the same computer he used to access AOL, Citibank's personal banking service, and other services. The investigation seems to have been delayed and perhaps limited as a result of Deutch's position.

It's old hat that personal computers (be they Windows, Macintosh, or UNIX-based) are inherently unsuitable for Multi-Level Security (MLS). What we see here is that even though all the proper procedures were in place, the human element is sufficient to undermine all of the technical controls. As long as we have people, we'll have RISKS!

Full article at <http://www.nytimes.com/yr/mo/day/news/washpol/cia-impeach-deutch.html>

[Multilevel security may not seem to be an issue here **internally** because John Deutch

had access to all of the information on his systems, considered as SYSTEM HIGH -- that is all logically at the highest level. However, surfing the (unclassified) Web is clearly a NO-NO from such a machine. RISKS readers are of course familiar with the risks of Web browsing. However, an added note in this case was the report that the visited sites included a porn site. Deutch apparently denied having accessed porn any sites, suggesting that it might have been done by one of his offspring? If that is indeed true, it would make the presence of highly classified information on a multiuser workstation even more untenable. (On one hand, even if such a PC claimed to be multilevel secure, that would be a VERY BAD misuse. On the other hand, RISKS readers know how one can be duped into visiting sites other than what was expected, as in clicking on whitehouse.com instead of whitehouse.gov, or in clicking on a Trojan-horsed URL.) PGN]

CERT Advisory CA-2000-02

CERT Advisory <cert-advisory@cert.org>
Wed, 2 Feb 2000 12:23:25 -0500 (EST)

CERT Advisory CA-2000-02
Malicious HTML Tags Embedded in Client Web Requests

This advisory is being published jointly by the CERT Coordination Center, DoD-CERT, the DoD Joint Task Force for Computer Network Defense (JTF-CND), the Federal Computer Incident Response Capability (FedCIRC), and the National Infrastructure Protection Center (NIPC).

Original release date: February 2, 2000
[Subsequently revised. Please pick up the latest version at <http://www.cert.org/advisories/CA-2000-02.html> and see http://www.cert.org/tech_tips/malicious_code_FAQ.html as well as a later note on disabling Java http://www.cert.org/tech_tips/malicious_code_FAQ.html#java. PGN]

Systems Affected

- * Web browsers
- * Web servers that dynamically generate pages based on

unvalidated
input

Overview

A web site may inadvertently include malicious HTML tags or script in a dynamically generated page based on unvalidated input from untrustworthy sources. This can be a problem when a web server does not adequately ensure that generated pages are properly encoded to prevent unintended execution of scripts, and when input is not validated to prevent malicious HTML from being presented to the user.

[This is referred to as "cross-site scripting". Note that executables in the URL itself can have nasty effects. PGN]

🔥 NSA system inoperative for four days

"Peter G. Neumann" <Neumann@CSL.sri.com>

Sun, 30 Jan 2000 04:31:15 -0500

For almost the entire work week of 24 Jan 2000, failures of NSA computers caused an information blackout for intercepted messages. The failure was blamed by one report on a ``system overload'', by another report on a software problem. [Sources: NSA System Inoperative for Four Days, by Walter Pincus, *The Washington Post*, 30 Jan 2000, Page A2, <http://www.washingtonpost.com/wp-dyn/articles/A49286-2000Jan29.html>; Kinder, gentler NSA admits human frailties, Thomas C. Greene, <http://www.theregister.co.uk/000131-000001.html>]

⚡ Leak lets 64 get rich quick

David Shaw <David.Shaw@alcatel.com.au>

Fri, 4 Feb 2000 11:54:27 +1100

On Wednesday, February 2, 2000, the Reserve Bank of Australia (RBA) formally announced an increase in the official interest rates of 0.5%.

The formal announcement was made at 09:30. However, in what turned out to be an embarrassing mistake for the RBA, 64 people were sent an e-mail at 09:24 (i.e., 6 minutes early) advising them of the rate increase. This was quite remarkable in itself, as the RBA has a near-legendary record of security.

The information proved to be very valuable for two reasons. Not only was the information available early to a very small segment of the market, the size of the rate increase was unexpected. Virtually the entire market had been expecting/predicting an increase of just 0.25%.

In the 6 minutes prior to 09:30, approximately AUD\$3 billion worth of bill and bond futures were dumped on the market.

The record of trades at the Sydney Futures Exchange demonstrates the selling frenzy. When interest rates last rose, on November 3, 1999, 336 three-year bond futures contracts and 324 90-day bank bill futures were traded between 09:25 and 09:30. The corresponding trades preceding yesterday's announcement were 2,739 and 2,811.

To quote an unnamed trader: "Some people made a lot of money in those few minutes."

Source: *Sydney Morning Herald* (www.smh.com.au). Thursday Feb 3, 2000.

David Shaw, Alcatel Australia Limited

david.shaw@alcatel.com.au

⚡ EFIS failure main suspect in Crossair crash

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Wed, 02 Feb 2000 11:07:21 +0100

Flight data displays such as airspeed and attitude indicators as well as navigation displays on modern commercial aircraft are nowadays electronic, replacing mechanical displays that were common until 10-15 years ago. Mechanical displays are often used as backup, although there are electronic backup displays available on the market. Mechanical displays were/are not susceptible to total outage. Airspeed indicators are basically differential barometers, and mechanical attitude indicators are gyroscopes.

According to Flight International's David Learmount (01-07.02.2000, p12), Electronic Flight Instrument System (EFIS) failure is the "main possibility" being looked at by the Swiss accident investigation people (BEAA) in the crash of the Crossair Saab 340B just after takeoff from Zuerich on 10 January. This was Crossair's first accident. I emphasise that the causes of the accident have not been established. It is hoped that the non-volatile memory on the EFIS displays can be recovered and read, to determine how what the pilots were seeing corresponds (or not!) with the flight profile recorded by the flight data recorder. (This is a benefit not provided by mechanical displays, although it would hardly make up for the susceptibility of EFIS to outages!)

EFIS failures have been noted in particular in incidents involving a Virgin A340 and a Martinair B767 (see the compendium Computer-Related Incidents With Commercial Aircraft on my WWW site). A Formosa Airlines Saab 340B descended into the ocean on 18 March 1998, and it has been rumored that one EFIS display was known before the flight not to be functioning.

Peter Ladkin, University of Bielefeld

<http://www.rvs.uni-bielefeld.de>

Terra spacecraft problems

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Wed, 12 Jan 2000 11:06:42 +0100

Flight International, 11-17 Jan 2000, p29, reports that NASA has fixed "computer and antenna faults" on the Terra spacecraft, launched 18 Dec 1999. Terra is part of the Earth Observing System. "The main computer shut down shortly after launch because of a bug in the navigation software, according to NASA." The failure occurred a minute before the winter solstice, while the sun's position in the nav software was being updated.

On the other side of things, the antenna "was repaired by alterations to the software", at which one can only marvel. Maybe Uri Geller is now programming for a living. Or maybe they meant the problem was worked around.

Peter Ladkin

ladkin@rvs.uni-bielefeld.de www.rvs.uni-bielefeld.de

⚡ Patients will be able to wear their hearts on the Internet

"NewsScan" <newsscan@newsscan.com>

Mon, 24 Jan 2000 09:25:03 -0700

In a venture with Microsoft and IBM, Minneapolis-based medical device company Medtronic will invest more than \$230 million to develop a system that will allow heart patients to send cardiac data to cardiologists via the Internet, from their homes or remote locations worldwide. The company's medtronic.com division will be the focal point of a new Patient Management Business. [<http://www.sjmercury.com/svtech/news/breaking/merc/docs/082323.htm>, Reuters in *San Jose Mercury News*, 24 Jan 2000, via NewsScan Daily, 24 Jan 2000]

[And what about the reverse direction? Would you like to have YOUR heart interactively controllable by doctors and insurance companies and everyone else on the Internet? PGN]

⚡ Yahoo suit compares cookies to stalking

"NewsScan" <newsscan@newsscan.com>

Mon, 31 Jan 2000 08:09:56 -0700

A lawsuit filed by Dallas-based Universal Image Inc. accuses Yahoo! of violating Texas law when it collects "cookies" from Web site visitors. "We think the court will declare the use of cookies illegal in Texas," says Universal attorney Lawrence Friedman. "It is electronic stalking. It violates the eavesdropping statutes, and from a civil aspect it's an invasion of privacy." Friedman says he plans to file a class-action lawsuit against the company. Meanwhile, DoubleClick was sued last week by a California woman who claims the online ad company illegally collected and sold her personal and demographic data. [ZDNet/MSNBC 28 Jan 2000] <http://www.msnbc.com/news/363455.asp>; NewsScan Daily, 31 Jan 2000]

⚡ China to require encryption information

"NewsScan" <newsscan@newsscan.com>

Tue, 25 Jan 2000 08:18:19 -0700

[On 31 Jan 2000] China's government plans to institute a rule requiring foreign firms in China to disclose what type of software they use for encrypting their electronic messages. Eventually, the companies must divulge details about employees using the software, making it easier for authorities to monitor personal and commercial Internet use. The new rules also bar Chinese companies from buying products containing foreign-designed encryption software, a move that could stymie the growth of Internet use in that country. Diplomatic missions are exempted, but the regulations cover the routers and servers that make up the backbone of China's networks, most of which came from foreign companies. "If IBM or Hewlett-Packard wants to sell an e-commerce Web server to China, it might have to isolate which parts relate to security" and find a Chinese company to write the software, says the director of the U.S. Information Technology Office's Beijing branch. "I don't think Chinese companies have that ability." [**Wall Street Journal**, 25 Jan 2000 <http://interactive.wsj.com/articles/SB948739893578536271.htm> via NewsScan Daily, 25 Jan 2000]

[According to later reports, very few are signing up. PGN]

🔥 Study criticizes health sites for privacy intrusions

"NewsScan" <newsscan@newsscan.com>

Wed, 02 Feb 2000 09:39:09 -0700

In a study conducted for the California HealthCare Foundation, the Georgetown University's Health Privacy Project has found that drkoop.com, webmd.com, ivillage.com, yahoo.com, onhealth.com, and other Web sites that provide information on health matters are cavalier about privacy practices: "The privacy policies of health Web sites do not match up with their own practices." Example: some companies share e-mail addresses and other visitor data even though their Web sites promised they would do no such thing. The companies are disputing the study findings. [Reuters/**San Jose Mercury News** 1 Feb 2000, <http://www.sjmercury.com/svtech/news/breaking/internet/docs/1603091.htm>; NewsScan Daily, 2 Feb 2000]

🔥 AT&T Business Internet Service DNS major outage 28 Jan 2000

"Randy Holcomb" <randy_holcomb@attglobal.net>

Fri, 28 Jan 2000 23:24:58 -0600

At 1400 EDT AT&T Business Internet Services (formerly IBM Global Network Internet Services) lost both primary and backup Domain Name Servers; resulting in the inability of AT&T Business Internet Customers to use the service.

The DNS's were back online a few minutes short of 2300 EDT.

✶ More risks with MS Outlook

Jason Axley <jason.axley@attws.com>

Tue, 1 Feb 2000 10:05:34 -0800 (PST)

The recent threads about information hiding in MS Outlook are quite timely as I've just recently discovered an interesting information hiding "feature" of MS Outlook.

I received an e-mail from an MS Outlook user that was transmitted to me via SMTP. The e-mail was in MIME multipart/alternative format and, as such, had two attachments: a plain text version of the e-mail content and another attachment with the exact same message in HTML format. Outlook has settings that let users control which format they sent Internet users e-mail in and this user has Outlook configured to send both versions (I believe that this is the default setting when sending to non-Exchange addresses).

I replied to this individual using Pine but then this individual responded saying that my message was received, but that there wasn't any additional text in it. I thought this strange as I can see in my sent-mail that I did reply with additional text. So, I sent the message again and again was told that there wasn't any text in the message.

It turns out that what was happening was that I had modified the plain text version of the multipart/alternative MIME message (which is the one that Pine opens as the actual message), but that when Pine sent the reply, it included the HTML "alternative" version as an attachment as well (although this was an alternative for the *original* message) Outlook then ignores the modified plain text version because it thinks that the attached HTML version is the same message, just in HTML. So, the recipient was seeing the original HTML message that I hadn't modified and was not able to see the plain text version. Outlook doesn't even list the plaintext version as an attachment so Outlook users cannot access the information there even if they wanted to!

Ironically, the text that Exchange or Outlook puts in the message header for non-MIME-compliant MUAs says "This message is in MIME format. Since your mail reader does not understand this format, some or all of this message may not be legible."

Jason AT&T Wireless Services, IT Security UNIX Security Operations Specialist

⚡ Who is at risk with this virus advertisement?

"R.S. \ (Bob\) Heuman" <rsh@idirect.com>

Sat, 29 Jan 2000 21:03:52 -0500

The following is a message I received via my subscription to this security jobs list. I have to wonder - if anyone answers it, what will happen... Will they get the job, or will they be investigated by the FBI, NSA, etc. I know that I would NOT answer it. Of course, I also have to wonder who the US Military will be targetting should they hire someone with the attributes desired. [Assuming they even can trust that individual...]

What next? What is the risk to the rest of us? Does anyone really think a security jobs listserve has only US subscribers?

R.S. (Bob) Heuman, Toronto, ON, Canada

```
> FROM: Drissel, James W. <james.drissel@CMET.AF.MIL>
> DATE: January 27, 2000 16:18
> TO: SECURITYJOBS@SECURITYFOCUS.COM <SECURITYJOBS@SECURITYFOCUS.COM>
```

```
> Subject: Virus coder wanted
```

```
> Computer Sciences Corporation in San Antonio, TX is looking
for a good
> virus coder. Applicants must be willing to work at Kelly AFB
in San
> Antonio. Other exploit experience is helpful.
```

```
> Send Resumes/questions to james.drissel@cmet.af.mil
```

[Although RISKS generally avoids running job ads, and especially

Advirusements, this one has some interesting RISKS-Related Ramifications.

R-R&R? PGN]

🔥 Organisms do not adapt to their environment!

"Bob Frankston" <rmf2gRisks@bobf.Frankston.com>

Mon, 31 Jan 2000 12:41:37 -0500

(Was: Lessons of Y2K, Toby Gottfried, [RISKS-20.77](#))

This is backwards?

ORGANISMS DO NOT ADAPT TO THEIR ENVIRONMENT. That is a fallacy called adaptionism!!!

Evolution works by not anticipating the need for solutions but having enough disparate solutions so that, given a problem, it's likely that there will be a solution that works.

This resiliency is the real reason that Y2K was a nonissue. Systems as brittle as the ones posited by the Y2K theorists don't work in practice and have largely been eliminated from the ecosystem. New brittleness will be discovered and some will be replaced by small scale alternatives and other failures may be larger scale.

The big danger is the hubris associated with the notion that we must have a vision to avoid pitfalls. Of course we shouldn't be stupid and should anticipate obvious problems. But it is far more important to assume that we will continue to be surprised and need to have enough "fat" available to survive problems.

It's also foolish to posit that we must model safety on static

systems and
limit our possibilities to what we can do unaided and
unenanced. If we
eschew mechanical aids, why should we be more tolerant of
cognitive aids
such as logic, reason and testing which often confound common
sense and
faith.

In nature (to personify emergent behavior) systems only function
in riskful
dynamic states. The static state for an organism or other
ecosystem is
called death. The conversion of necessities into luxuries is
most natural.
Skin, for example, is no longer an option.

Nature can't be fooled but we can do a fine job in deluding
ourselves.

Fatal Words

"Bob Frankston" <rmf2gOther@bobf.Frankston.com>
Sun, 6 Feb 2000 01:54:47 -0500

In an essay I'm writing, I was reminded of the book **Fatal
Words** by Steven
Cushing [ISBN 0-226-13201-3]. It's about misunderstandings
between pilots
and instructions from the ground and other consequences of the
World War II
communications and avionics still in use. A great example of
what happens
when certification and irrational fear of risk prevent
improvements in
technology and safety.

Bob Frankston <http://www.Frankston.com>

⚡ abcnews.com manually updates copyright year

David Glicksberg <davidg@bourbaki.jpl.nasa.gov>

Wed, 2 Feb 2000 21:01:17 -0800 (PST)

Articles written during the first week or so of 2000 on abcnews.com have

a misdated notice at the bottom of the page: "Copyright (C)1999 ABC

News Internet Ventures." However, the dateline (which shows the place,

month, and day, but usually omits the year) and the URL (which has an

embedded date of the form YYMMDD) together clearly mark the article's

date. One can still view articles exhibiting this glitch, for example:

http://www.abcnews.go.com/sections/science/DailyNews/clone_cells000105.html

I notified abcnews.com Tech Support on January 6, and within several days,

all new articles had the correct copyright year. This leads me to believe

that abcnews.com may use a hardcoded copyright year, which someone forgot

to update in a timely fashion.

I wonder how many programs and systems out there require manual year

rollover ... in this case, the slipup was of little consequence.

Dave Glicksberg -- glicksbergd@acm.org

⚡ People For Internet Responsibility issues and status report

Lauren Weinstein; PRIVACY Forum Moderator <lauren@vortex.com>

Sat, 5 Feb 2000 21:15 PST

Greetings. The current version of the PFIR (People For Internet Responsibility) "Issues" document, and a status report regarding PFIR activities, are now available via the PFIR Web site at:

<http://www.pfir.org>

The issues document covers a wide range of important Internet and Web topics.

It is (and will continue to be) a work in progress, and while quite comprehensive is undergoing rapid expansion. Many of the topics relate to privacy issues, technology risks, and other matters that should be of interest to current and potential Internet users.

Your input and comments regarding both of these documents would be very much appreciated via the e-mail addresses indicated within the docs themselves.

Thanks very much.

--Lauren--

lauren@vortex.com

Lauren Weinstein

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

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

Member, ACM Committee on Computers and Public Policy

⚡ New Security Paradigms Workshop 2000: Call For Papers

Crispin Cowan <crispin@wirex.com>

Sat, 29 Jan 2000 03:34:42 +0000

Call For Papers
New Security Paradigms Workshop 2000
An ACM/SIGSAC sponsored workshop
19 - 21 September 2000
Ballycotton, County Cork, Ireland
<http://www.nspw.org/>

[This is a very small but remarkably insightful workshop, in its 8th year.

Registration is limited by acceptance of submitted papers and justifications for why you should attend. If you wish to participate,

FIRST contact both Program Chairs -- Cristina Serban (cserban@att.com)

and Brenda Timmerman (btimmer@ecs.csun.edu) soon. Final submissions are

due toward the end of March. Some further information will be emerging at

<http://www.nspw.org/> . 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 20: Issue 79

Tuesday 15 February 2000

Contents

- [Distributed denial-of-service attacks](#)
[PGN](#)
- [PFIR Statement on Recent Internet Denial of Service Attacks](#)
[Lauren Weinstein](#)
- [Risks of bouncing messages from closed e-mail lists](#)
[Mich Kabay](#)
- [My.MP3.com and the Beam-it protocol](#)
[Dan Wallach](#)
- [Re: Organisms don't adapt????](#)
[Bob Blakley](#)
[Gordon Foreman](#)
- [More risks with MS Outlook](#)
[kclemson](#)
- [Review of "Database Nation"](#)
[Gene Spafford](#)
- [Info on RISKS \(comp.risks\)](#)

⚡ **Distributed denial-of-service attacks**

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

Mon, 14 Feb 2000 08:17:12 PST

The previous week saw three days of distributed denial-of-service (DDoS) attacks, disabling Yahoo, Amazon, eBay, CNN.com, Buy.com, ZDNet, E*Trade, and Excite.com for a few hours each. The flooding attacks were triggered from a variety of unknowing intermediate zombie systems that had been penetrated, although the launched DDoS attacks required no penetrations of their target systems.

The events should be no surprise to RISKS readers. The likelihood of such attacks has been discussed for a long time, and scripts (such as Trinoo, Tribal Flood Network TFN and TFN2K, and Stacheldraht -- German for barbed wire) have been available as well. It may seem unnecessary for me to note here that our information infrastructures are riddled with vulnerabilities that made these attacks easy to carry out, but that is simply the way it is.

The media had a field day with talking heads, soundbites, one-line quotes, speculations, and very little hard information on what techniques were used and who was responsible.

I have just finished my April 2000 Inside Risks column for the Communication of the ACM on this subject, although it is clearly not an April Fool's joke. The column will appear on my Website shortly before 1 April, but I won't replicate it here.

The following note from Lauren Weinstein was distributed to the

PFIR mailing

list. In general, RISKS will not reproduce PFIR messages, to avoid undesired duplication for readers of both lists. However, this particular message saves me the trouble of trying to PGN-ed-itorialize on all of the recent media reports in what is still an ongoing saga. Besides, [RISKS-20.79](#) has been pending for too long already.

✶ PFIR Statement on Recent Internet Denial of Service Attacks

PFIR - People For Internet Responsibility <pfir@pfir.org>

Wed, 9 Feb 2000 21:34:09 -0800 (PST)

PFIR Statement on Recent Internet Denial of Service Attacks

(<http://www.pfir.org/statements/02.09.00>)

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

Greetings. The recent rash of "Denial of Service" (DoS) attacks on major Internet sites such as Yahoo!, E-Bay, CNN, and others, has caused outcries of surprise and consternation in many quarters, and has become the lead story for many newscasts. But these attacks come as no surprise to many of us, who have long predicted that these sorts of events would come to pass.

It's basically easy to understand. Imagine a small firm with two phone lines. Now have 10,000 people at pay phones scattered around the world all trying to call that company at once, and hanging up as soon as there is an

answer. Few (if any) customer calls will get through, and finding the perpetrators will be problematic at best.

A variety of software tools are available for launching effectively anonymous DoS attacks on the Internet, which in many cases may involve otherwise innocent computers "hijacked" for this purpose. While some of the simpler attack methods may be repelled to a degree by "filtering" to block some of the offending data, the fundamental structure of the existing Internet makes complete solutions essentially impossible. We can expect to see a rapid evolution in the sophistication of such attacks and their relative invulnerability to quick eradication. There will not be simple answers of any lasting value.

There are a number of very important lessons to be learned from these events. It seems apparent that the rush to move all manner of important or even critical commercial, medical, government, and other applications onto the Internet and Web has far outstripped the underlying reality of the existing Internet infrastructure.

Compared with the overall robustness of the U.S. telephone system, the Internet is a second-class citizen when it comes to these kinds of vulnerabilities. Nor will simply throwing money at the Internet necessarily do much good in this regard. More bandwidth, additional servers, and faster routers--they'd still be open to sophisticated (and even not so sophisticated) attacks which could be triggered from one PC anywhere in the

world.

In the long run, major alterations will be needed in the fundamental structure of the Internet to even begin to get a handle on these sorts of problems, and a practical path to that goal still remains fuzzy at this time.

For now, it might be advisable for everyone to remember that the Internet, for all its wonders, is in many ways very fragile. We must not allow ourselves to get into a position where being cut off from a site for a few hours--or even longer--puts people or property at risk. Our lives should not revolve around guaranteed 24/7 access to E-Bay, or Yahoo!, or *any* site on the public Internet, regardless of its importance. The need for alternative access methods for critical systems, and the potential recklessness of eliminating older systems in exchange for 100% Internet dependence, cannot be overstated.

The current attacks are sure to be but the beginning. Many even more attractive targets are likely to be appearing that will draw ever more sophisticated fire. Imagine what a concerted denial of service attack might do to an election with Internet/Web-based voting--a technology being pushed on a fast track in many quarters.

It's time to get past the "dot com" hype and to start considering carefully the realities, and limits, of the technology on which we're trying to base so much, so very fast. If we continue to plow ahead without heeding these

lessons, it will be at our extreme peril.

Lauren Weinstein <lauren@vortex.com>

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

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

Member, ACM Committee on Computers and Public Policy

⚡ Risks of bouncing messages from closed e-mail lists

Mich Kabay <mkabay@compuserve.com>

Mon, 14 Feb 2000 12:27:57 -0500

I have noticed that a junk e-mailer has taken to using a closed mailing-list server as a relay for his unauthorized messages.

The scam works like this:

- 1) Criminal locates a closed mailing list that responds to unauthorized postings by sending back an automated rejection notice that includes the original message.
- 2) Criminal sends junk e-mail to the closed list using the desired `_target's_` e-mail addresses in forged header.
- 3) Closed list obligingly bounces the original message back to the target's address.

Authorized users of the closed list do not need to receive a message informing them that their messages have not been accepted (presumably due to some oversight or glitch) because they will likely note the absence of their

message on the list anyway.

Unauthorized users of the list do not need to see the text of their message at all in their electronic rejection note -- a stock reply explaining how to gain admission to the list is more relevant.

Therefore I recommend that at the very least, administrators for closed e-mail lists prevent their listserv from sending the _complete text_ of a bounced message back to the supposed originator.

However, there is a more serious vulnerability here: infinite loops between two or more closed lists.

If an attacker forges the originating address of a closed list that sends back automated rejection notes to another closed list that sends back automated rejection notes, then each forged message will generate a mailstorm as a function of the speed of the servers in sending bounce messages to each other. The chain can be extended to multiple closed-list servers, causing even more useless traffic and potentially contributing to denial of service for the legitimate users of the closed lists.

RECOMMENDATIONS:

A) Turn off automated notification of rejection altogether on all closed lists; or if you feel that the notification messages are important, then

B) Configure the listserv to send back only the title of a rejected message, not the complete text; or if you feel like addressing the potential

vulnerability head-on,

C) Design a check of a log file so that the listserv for a closed list can quickly identify a mailstorm and stop it by turning off automated notification of rejection when it is being abused.

M. E. Kabay, PhD, CISSP, Security Leader, Information Security Group
Adario, Inc., 255 Flood Road, Barre, VT 05641-4060
+1.802.479.7937

[NOTE the push-pull duality between a mailstorm and a maelstrom.

A mailstorm pushes things in, whereas a maelstrom pulls them in. PGN]

⚡ My.MP3.com and the Beam-it protocol

Dan Wallach <dwallach@cs.rice.edu>
Fri, 11 Feb 2000 15:59:01 -0600

Last week, MP3.com released a version of its Beam-it system for Linux. This is a system meant to allow you to "beam" your audio CDs to the MP3.com server, which would then provide them back to you as streaming MP3 files. Because only a small amount of data is actually transmitted during the protocol, this is touted as an efficient and novel network service. MP3.com already has the music on its servers. "Beaming" is really proving you own a CD, and thus MP3.com feels safe putting a reference to it in your online account.

The RIAA (Recording Industry Association of America) has other thoughts on

the matter, and is currently engaged in some testy litigation with MP3.com.

Meanwhile, the service continues to run.

On 4 Feb 2000, MP3.com posted a Linux version of their Beam-it client software and took the unusual step of releasing *most* of it as free source, with a small closed source pre-compiled component. In addition to some posters on Slashdot, we reverse engineered this module and studied the protocol. MP3.com did a reasonable job. It's unlikely you'll successfully "beam" a music CD to them unless you are physically holding the CD (or a bit-for-bit copy of it). Aside from this, there are still some privacy concerns about their system. It's also completely trivial for users to share accounts (which might be a concern for the RIAA).

For those interested in more details:

<http://www.cs.rice.edu/~dwallach/pub/beam-it.html>

Dan Wallach, Rice University

✶ Re: Organisms don't adapt???? (Frankston, [RISKS-20.78](#))

"Bob Blakley" <bob_blakley@hotmail.com>

Wed, 09 Feb 2000 17:19:24 CST

Sorry to be difficult, but organisms clearly do adapt to their environment, both behaviorally (build houses, e.g.) and physically (e.g. grow thicker fur in the winter, suntan, etc...).

But this isn't the basis of evolution of species - which is due

to
populations adapting to their environment by virtue of well-
adapted
individuals reproducing at differentially higher rates than
poorly adapted
individuals.

Bob Blakley, Chief Scientist, Tivoli SecureWay Business Unit

✦ Re: Organisms don't adapt???? (Frankston, [RISKS-20.78](#))

Gordon Foreman <gforeman@lanl.gov>

Mon, 07 Feb 2000 17:04:11 -0700

I think you meant the opposite!

In nature (to personify emergent behavior) systems only function
in riskful
dynamic states. The static state for an organism or other
ecosystem is
called death. The conversion of necessities into luxuries is
most natural.
Skin, for example, is no longer an option.

I think you meant to say the conversion of luxuries into
necessities is
most natural, as yesterday's luxuries are nearly always today's
necessities.

Gordon Foreman, Los Alamos National Laboratory 505-667-3368
phone

✦ More risks with MS Outlook (Axley, [RISKS-20.78](#))

<kclemsom@my-deja.com>

Wed, 09 Feb 2000 21:05:48 GMT

I just tried it with netscape and OE and got the same result. The bug is with pine -- it returns multipart/alternative and should have returned multipart/mixed.

The multipart/alternative means that the sending client is guaranteeing that the body portions are exactly equivalent, and so clients that understand the higher level text (html), are free to throw away the downlevel text (plain text). But since pine edited the text/plain part, it made the body parts unequivalent but other clients that follow the RFC throw away the part they don't need.

Neither outlook nor any other HTML aware client should ever show an attachment for the plain text body part on a multipart/alternative message - that would defeat part of the purpose of that content type.

I will report the bug to the pine authors. Next time you should be more careful when pointing fingers.

[ZDNet.com/zdnn/stories/news reports that Windows 2000 apparently has about 63,000 defects, although later comments suggest under half of those are significant. PGN]

⚡ Review of "Database Nation"

Gene Spafford <spaf@cerias.purdue.edu>
Mon, 7 Feb 2000 08:10:58 -0500

"Database Nation: The Death of Privacy in the 21st Century"

by Simson Garfinkel

O'Reilly & Associates, 2000

ISBN 1-56592-653-6

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

First, of all, I should disclose what is probably a conflict of interest.

Simson and I have been friends for years, and we have collaborated on a

number of projects, including 3 books. As such, some people (who don't know

me well) might suspect that I wouldn't provide an objective review. So, if

you think that might be the case, then discount my recommendation by half --

and still buy and read this book. Simson has done an outstanding job

documenting and describing a set of issues that a great many people --

myself included -- believe will influence computing, e-commerce, law and

public policy in the next decade. They also impact every person in modern

society.

This book describes -- well, and with numerous citations -- how our privacy

as individuals and members of groups has been eroding.

Unfortunately, that

erosion is accelerating, and those of us involved with information

technology are a significant factor in that trend. Credit bureaus

accumulate information on our spending, governments record the minutiae of

their citizens' lives, health insurance organizations record everything

about us that might prove useful to deny our claims, and merchants suck up

every bit of information they can find so as to target us for more

marketing. In each case, there is a seemingly valid reason, but

the accumulated weight of all this record-keeping -- especially when coupled with the sale and interchange of the data -- is frightening. Simson provides numerous examples and case studies showing how our privacy is incrementally disappearing as more data is captured in databases large and small.

The book includes chapters on a wide range of privacy-related issues, including medical information privacy, purchasing patterns and affinity programs, on-line monitoring, credit bureaus, genetic testing, government record-keeping and regulation, terrorism and law enforcement monitoring, biometrics and identification, ownership of personal information, and AI-based information modeling and collection. The 270 pages of text present a sweeping view of the various assaults on our privacy in day-to-day life. Each instance is documented as a case where someone has a reasonable cause to collect and use the information, whether for law enforcement, medical research, or government cost-saving. Unfortunately, the reality is that most of those scenarios are then extended to where the information is misused, misapplied, or combined with other information to create unexpected and unwanted intrusions.

Despite my overall enthusiasm, I was a little disappointed in a few minor respects with the book. Although Simson concludes the book with an interesting agenda of issues that should be pursued in the interests of

privacy protection, he misses a number of opportunities to provide the reader with information on how to better his or her own control over personal information. For instance, he describes the opt-out program for direct marketing, but doesn't provide the details of how the reader can do this; Simson recounts that people are able to get their credit records or medical records from MIB, but then doesn't provide any information on how to get them or who to contact; and although he sets forth a legislative agenda for government, he fails to note realistic steps that the reader can take to help move that agenda forward. I suspect that many people will finish reading this book with a strong sense of wanting to *do* something, but they will not have any guidance as to where to go or who to talk with.

The book has over 20 pages of comprehensive endnotes and WWW references for the reader interested in further details. These URLs do include pointers to many important sources of information on privacy and law, but with a few puzzling omissions: I didn't see references to resources such as EPIC or Lauren Weinstein's Privacy Digest outside of the fine print in the endnotes. I also didn't note references to ACM's Computers, Freedom and Privacy conferences, the USACM, or a number of other useful venues and supporters of privacy and advocacy. Robert Ellis Smith's "Privacy Journal" is mentioned in the text, but there is no information given as to how to subscribe to it. And so on.

I also noted that the book doesn't really discuss much of the

international
privacy scene, including issues of law and culture that
complicate our
domestic solutions. However, the book is intended for a U.S.
audience, so
this is somewhat understandable. A few other topics -- such as
workplace
monitoring -- are similarly given more abbreviated coverage than
every
reader might wish. Overall, I recognized few of those.

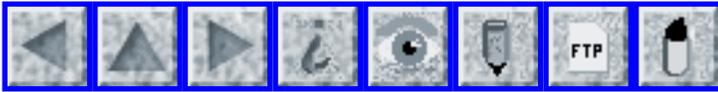
On the plus side, the book is very readable, with great examples
and
anecdotes, and a clear sense of urgency. Although it is obvious
that Simson
is not an impartial party on these topics, he does present many
of the
conflicting viewpoints to illustrate the complexity of the
issues. For
instance, he presents data on the need for wiretaps and criminal
investigation, along with accounts and descriptions of
bioterrorism,
including interviews with FBI officials, to illustrate why there
are people
of good faith who want to be able to monitor telephone
conversations and
e-mail. If anything, this increases the impact of the book --
it is not an
account of bad people with evil intent, but a description of
what happens
when ideas reasonable to a small group have consequences beyond
their
imagining -- or immediate concern. The death of privacy is one
of a
thousand cuts, each one small and seemingly made for a good
reason.

Simson has committed to adding important information to the WWW
site for the
book. Many (or most) of the items I have noted above will
likely be
addressed at the WWW site before long. Simson also has informed
me that the

publisher will be making corrections and some additions to future editions of the book if he deems them important. This is great news for those of us who will use the book as an classroom text, or if we recommend the book to policy makers on an on-going basis. Those of us with older copies will need to keep the URL on our bookmark list.

Overall, I was very pleased with the book. I read it all in one sitting, on a flight cross-country, and found it an easy read. I have long been interested in (and involved in) activities in protection of privacy, so I have seen and read most of the sources Simson references. Still, I learned a number of things from reading the book that I didn't already know -- Simson has done a fine job of presenting historical and ancillary context to his narrative without appearing overly pedantic.

This is a book I intend to recommend to all of my graduate students and colleagues. I wish only there was some way to get all of our elected officials to read it, too. I believe that everyone who values some sense of private life should be aware of these issues, and this book is a great way to learn about them. I suggest you go out and buy a copy -- but pay in cash instead of with a credit card, take mass transit to the store instead of your personal auto, and don't look directly into the video cameras behind the checkout counter. Once you read the book, you'll be glad you did.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 80

Sunday 20 February 2000

Contents

- [EPA web site shut down](#)
[Rick Blum](#)
- [Online prankster distorts Clinton chat](#)
[NewsScan](#)
- [Computer glitch cancels 86 America West flights](#)
[George Dinwiddie](#)
- [Fire takes out Nottingham Phones](#)
[Dave Weingart](#)
- [Breach exposes H&R Block customers' tax records](#)
[George Dinwiddie](#)
- [Great West gives out too much personal info](#)
[Taylor Hutt](#)
- [YAIESB: Yet Another Internet Explorer Security Bug](#)
[Jeremy Epstein](#)
- [Re: Distributed denial-of-service attacks](#)
[Ken Cox](#)
- [Re: Win 2000 63,000 Bugs](#)
[Jim Allchin via Chris Smith](#)
- [REVIEW: "Virtual Private Networking", Bruce Perlmutter/Jonathan Zarkower](#)
[Rob Slade](#)

- [CFP: Safety & Reliability of embedded Software Systems](#)
[Pete Mellor](#)
 - [USENIX Annual Technical Conference, 2000 - Preliminary Program](#)
[Moun Chau](#)
 - [Information Survivability Workshop ISW 2000](#)
[Howard Lipson](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ EPA web site shut down

"Rick Blum" <blumr@ombwatch.org>

Fri, 18 Feb 2000 15:38:58 -0500

[via Dave Farber <farber@cis.upenn.edu>... Many thanks to Dave's IP! PGN]

> Late Wednesday night EPA shut down its entire Internet services, including
> its web site and staff email.

> Our conclusion is that there is no rationale for the unprecedented
> shutting down of the EPA web site and email services, cutting off a major
> means for the public to communicate with EPA. There is no question that
> EPA has computer vulnerabilities, but these could have been resolved with
> good computer management. In the meantime, Rep. Bliley (R-VA), the chair
> of the House Commerce Committee, basically held a gun to EPA's head,
> effectively telling EPA to shut down its site or it would put information
> out about security risks, making it easier for the public to hack EPA's
> site, instead of helping EPA make fixes. This does not exonerate EPA.

> EPA has known about its computer vulnerabilities for some time and has
> done little to fix the problems. Despite the computer problems at EPA,
> there was no "crisis." The General Accounting Office never recommended
> shutting down the EPA site, but Bliley, who has done the bidding of
> powerful special interests, has acted to thwart public access.

> THE STORY:

> Some months ago Rep. Thomas Bliley (R-VA), the chair of the House Commerce
> Committee, requested the General Accounting Office (GAO) to do a computer
> security audit at EPA. As the audit was coming to a close, GAO was
> required to share the information with EPA. But, reportedly, Bliley was
> upset since he didn't want EPA fixing the problems. Rather, he wanted to
> bash EPA. He required GAO to give him a copy of the letter to EPA and
> then, it is rumored, he leaked some portions to the press, making the
> problems at EPA sound horrendous.

> GAO did, however, find "serious and pervasive problems that essentially
> render EPA's agency-wide information security program ineffective." The
> problems at EPA mostly dealt with bad to poor computer management:
> ineffective firewalls; lack of controls (e.g., passwords); logs that
> didn't capture hackers; computer doors that had been left open. GAO found
> EPA's "vulnerabilities...have been exploited by both external and internal
> sources." It appears that GAO was able to take control of the router and
> then capture the password of anyone logging on to the system.

- > GAO does not have evidence of data being tampered with or violations of
- > trade secrets or enforcement data. In some cases where there were
- > violations, it resulted in criminal investigations. And while there are
- > big problems, GAO never recommended that EPA shut its web site down. (In
- > fact, GAO has found computer security problems at other agencies, such as
- > State Dept, but it appears no agency has completely and this thoroughly
- > cut off its Internet connection and email services.)

- > Bliley planned a hearing today (2/17) on EPA computer security and had
- > asked GAO to testify. EPA raised concerns about holding the hearing.
- > Reportedly, Bliley gave EPA an ultimatum: shut down the EPA web site and
- > all email services or the public would hear about how to hack the EPA web
- > site. EPA decided to shut down their Internet services last night.

- > Bliley postponed the hearing but called a press conference at 1 p.m. on
- > Friday. At the press conference, Bliley released the GAO testimony and
- > supported EPA's decision to shut down the web site. EPA claims it was
- > disappointed that it had to shut down.

- > According to folks in the White House, EPA is quickly trying to put the
- > public web site back up and sever its connection to the internal systems.
- > It is not clear when this will happen.

- > There are many issues that this "crisis" raises, but two stick out.

- > First, if EPA had security violations, why didn't Bliley give

EPA the time

> that is needed to fix the problems that GAO found? Why did he hold a gun

> to EPA's head? Even if there were computer security problems, it could

> have been handled in a manner that did not disrupt public access to the

> agency and did not create a "crisis."

> This raises questions about Bliley's objectives. Maybe it is a coincidence that a number of his campaign contributors are regulated by

> EPA. For example, a large grouping of contributors are from the mining

> and electrical gas sectors, which for the first time will need to report

> to EPA on toxic releases. Some of his larger contributors are listed as

> major polluters. Bliley is the same person who pushed the terrorism

> argument last summer as a reason to withhold public access to information

> about chemical hazards in our communities. Instead of improving public

> access, Bliley has taken a course of thwarting EPA and, hence, public

> access.

> Second, EPA has known for many years that it has computer management

> problems. Inspector General reports since 1997 have raised concerns, but

> little has been done to fix the problems. When GAO showed EPA it had

> problems, why didn't it immediately address these problems?

> EPA Administrator Browner took the helpful step to create an Information

> Office within EPA. But since then no one has been appointed to run the

> office. Increasingly, the Office is proving to be less than useful, maybe

> even a major disappointment. Why has the Office not taken the

leadership

> to develop a comprehensive information plan that covers
computer

> management issues?

> Rick Blum P: (202) 234-8494

> OMB Watch (CFC #0889) F: (202) 234-8584

> 1742 Connecticut Ave NW Em: blumr@ombwatch.org

> Washington, DC 20009-1171

> Web: ombwatch.org

> Right-To-Know Network: www.rtk.net

🔥 Online prankster distorts Clinton chat

"NewsScan" <newsscan@newsscan.com>

Thu, 17 Feb 2000 08:51:31 -0700

In what was billed as the first live online interview with a
sitting U.S.

president, CNN's chat with President Clinton turned kinky when a
computer

security consultant assumed Clinton's identity and changed his
response to:

"Personally, I would like to see more porn on the Internet." The
consultant

said guessing the president's nickname was an "easy trick," and
that "I hope

this harmless prank has served to let CNN know that this system
is insecure

and needs to be overhauled before someone does actual harm to
them or one of

their guests." Such security flaws can easily sabotage New Media
journalism

if not fixed, he added. [CBC News 16 Feb 2000

[http://cbc.ca/cgi-bin/templates/NWview.cgi?/news/2000/02/15/
online000215](http://cbc.ca/cgi-bin/templates/NWview.cgi?/news/2000/02/15/online000215);

included in RISKS with permission from NewsScan Daily, 17 Feb
2000.

NewsScan Daily is underwritten by IEEE Computer Society and

Arthur Andersen,
world-class organizations making significant and sustained
contributions to
the effective management and appropriate use of information
technology. NSD
is written by John Gehl and Suzanne Douglas, editors@NewsScan.
com.]

✶ Computer glitch cancels 86 America West flights

"Dinwiddie, George" <George.Dinwiddie@arbitron.com>
Fri, 18 Feb 2000 13:04:21 -0500

On 17-18 Feb 2000, America West Airlines canceled 86 flights,
due to the
failure of their flight-plan computer system. (Associated Press
item, 18
Feb 2000; PGN-ed)

[This seems like a major consequence for a relatively minor
system. GD]

✶ Fire takes out Nottingham Phones

Dave Weingart <dweingart@chi.com>
Thu, 17 Feb 2000 16:41:59 -0500

A fire in a switching station interrupted phone service for
large portions
of NTL's phone customers in Nottingham, England from 7pm on 16
Feb 2000
through most of 17 Feb 2000.

Dave Weingart, Randstad North America <dweingart@chi.com> 1-516-
682-1470

⚡ Breach exposes H&R Block customers' tax records

"Dinwiddie, George" <George.Dinwiddie@arbitron.com>

Wed, 16 Feb 2000 13:01:52 -0500

CNET reported that H&R Block's online tax-filing service exposed at least 50

customers' sensitive financial records to other customers over the weekend

of 12-13 Feb, prompting the company to shut down the system on 15 Feb.

Web-based registered users signing on were given access to someone else's

data. This was the second time in two weeks that H&R Block's widely used

"Do-it-yourself" Net filing service had to be shut down.

[Source: Courtney

Macavinta <courtm@cnet.com>, CNET News.com, 15 Feb 2000, URL:

<http://news.cnet.com/category/0-1005-200-1550948.html>, PGN-ed]

[The risks are obvious. The safeguard is less so. Certainly civil or

criminal penalties cannot prevent errors. GD]

⚡ Great West gives out too much personal info

Taylor Hutt <t.hutt@worldnet.att.net>

Tue, 15 Feb 2000 22:56:00 -0800

I recently changed jobs and moved, so I called my previous employer to give

them my new address. They said they would also tell Great West (401K

company; 'individual retirement plan' to people outside the US) about the

change of address.

Yesterday I got snail mail from Great West; a confirmation of my account imploring me to examine the information carefully and report any errors to them. I guess this is their odd 'change of address' confirmation.

Unfortunately the mail they sent me contains: my name, birthdate, social security number (SSN), sex, marital status, account number, the mutual funds to which I have made contributions - and the percentages of the contributions.

I called the 800 number to complain about their appalling lack of security for personal information and was greeted by a telephone system which said I could gain online access by pressing '2' - which I did. I was then asked to enter my SSN, which I did - and was then told that a PIN would be mailed to me. I wasn't required to confirm anything (not that it would have mattered, because I had all the confirmation information right at my fingertips). Following this, as most automated systems do, it hung up on me.

I then called back and got to speak with a customer service representative; I briefly told him why I was calling and then he had the audacity to tell me he wanted to confirm some information - my name, birthdate and SSN!

I was able to talk with the account representative for the company where I previously worked and she didn't seem to see the gravity of the situation, so I eventually got to speak with her boss, Nancy Lynch.

Nancy seemed more appreciative of my concerns and said she would

bring this
up in a meeting scheduled for 2000.02.21 and call me back. From
what I
gather, no one at this company has even thought about these
issues before -
which scares the hell out of me when I think about the amount of
money they
must be maintaining. I was assured that online access to my
account would
not allow any transfers out of the account, but heck... who
needs online
access when Great West will gladly send the key (i.e. all the
confirmation
information) to the intruder's mailbox! If I maliciously
changed someone
else's address, I could gain access to their account through the
phone
system and presumably cash out their account without them even
knowing it.

I wonder what other privacy gems are lurking out there with
financial
companies!

t.hutt@world.net.att.net

⚡ YAIESB: Yet Another Internet Explorer Security Bug

"Jeremy Epstein" <jepstein@webmethods.com>

Thu, 17 Feb 2000 09:28:42 -0500

Under certain circumstances, a web server can force an IE client
to serve up
the contents of a file on a local hard drive. The server needs
to
know/guess the name of the file to be retrieved. The
vulnerability only
exists if you have Active Scripting available for the security
zone (yet
another reason to turn it off!)

MS says "The vulnerability exists because it is possible, under very specific conditions, to violate IE's cross-domain security model in order to allow a web site to read data that it should be prevented from reading."

An interesting feature is that if you try to install the patch on a machine running IE 4.01 with SP1, the install states that the patch isn't needed (when in fact it really is). The only solution is to "upgrade" to a newer version of IE. Although MS warns of this on their web page, I wonder how many people will get a false sense of security when told they don't need the security patch.

See <http://www.microsoft.com/technet/security/bulletin/ms00-009.asp>

--Jeremy

🔥 Re: Distributed denial-of-service attacks ([RISKS-20.79](#))

"Ken Cox (11359)" <kcc@research.bell-labs.com>

Wed, 16 Feb 2000 13:41:09 -0600

I heard more than one reader pronounce "DoS" to rhyme with "sauce" -- and sound just like "DOS". I can only imagine the confusion that this caused with listeners.

The risk? One might argue this shows a lack of technical education in the media. But an equally strong argument can be made that the

fault lies with
the composers of the news releases, for not explaining the
jargon -- or
maybe even for not realizing that this is jargon, and not common
knowledge.

Ken Cox

kcc@research.bell-labs.com

✶ Re: Win 2000 63,000 Bugs

Chris Smith <chris@realcomputerguy.com>

Tue, 15 Feb 2000 23:10:02 -0500

And there's always the other side [Re: ZDNet comment in [RISKS-20.79](#)]:

> An Open Letter to Microsoft Customers on Windows 2000
> From: Jim Allchin, Group Vice President, Platforms Group,
Microsoft Corporation

You may have seen reports in the media claiming that Windows 2000 contains over 63,000 defects. I'd like to assure our customers that these reports are inaccurate. Microsoft is committed to delivering high quality products, and we believe Windows 2000 is the most reliable operating system Microsoft has ever shipped.

In fact, the technical press, industry analysts, and our customers have already spoken.

a.. There have been more than 20 technical reviews of Windows 2000, and in all of them Windows 2000 received very high marks in the area of reliability.

b.. Analyst studies show Windows 2000 to be significantly more reliable than any previous version of Windows ever.

c.. To ensure we received the maximum testing coverage possible before releasing we shipped over 750,000 beta test copies of Windows 2000.

d.. Many small businesses like CenterBeam and WFofR as well as hundreds of enterprises such as Ford, Wells Fargo, Motorola, and Prudential are currently rolling out Windows 2000 across their infrastructure.

e.. Windows 2000 has now been fully deployed in many businesses including Stride Rite and Sears Homelife.

f.. Additionally, Windows 2000 is driving many of the world's major websites, including Buy.com, Barnesandnoble.com, Dell.com, Microsoft.com, Monster.com and large ISPs such as DataReturn, and Digex.

So does Windows 2000 have 63,000 defects? The answer is a flat no. There was an internal development paper that described a broad set of focus areas for the team that mentioned the 63,000 number. However, without understanding our development process (which isn't described in this paper) reporting such a number is totally meaningless when taken out of context.

First, we track many issues internally in our "bug" database, including feature requests that someone may have mentioned or dreamed about, potentially confusing phrases in the documentation, performance improvement ideas, etc. - most of which are clearly not bugs in the classical sense. We track virtually everything mentioned by testers (internally or externally). These include feature requests, potential problems, or real problems. We also track any place in our code where we think we can improve an algorithm. This does NOT mean that there is a bug. In fact, it is often

the case the code is marked so that it can be reviewed in the future for performance or feature enhancements.

We also have a special advanced source code analyzer that we use. This tool generates a significant number of false positives (it thinks the code should be changed, but in fact it should not be). But, we track them all. The only way to be sure is to look at each hit and see if the issue is real or not. We love this tool. It helps us improve our code for readability and it can find bugs that our testing may not find. We also track our test code. There are over 10 million lines of test code that can also have improvements, potential bugs, etc. that we track in the same database. So, we track together test code, shipping code, and future code for the next release (we always have future projects cranking out code long before the previous release ships). Technically, we keep all of this information in a single tracking system and simply query for the kinds of information we want. At the end of every release we need to clean up our database and code since it ends up accumulating lots of random data. The internal paper discussed doing this clean up.

Will customers run into bugs in Windows 2000? We worked harder than ever to ensure they would not. Windows 2000 is the highest quality product we have ever released-just ask any one of the thousands of satisfied users who have experienced Windows 2000 so far.

We are very proud of Windows 2000's quality and our relentless pursuit of the highest quality software in the world.

Thank You,

Jim Allchin
Group Vice President, Platforms Group
Microsoft Corporation

⚡ REVIEW: "Virtual Private Networking", Bruce Perlmutter/ Jonathan Zarkower

"Rob Slade" <rslade@sprint.ca>
Wed, 16 Feb 2000 20:51:41 -0800

BKVRPRNG.RVW 20000111

"Virtual Private Networking", Bruce Perlmutter/Jonathan Zarkower,
2000, 0-13-020335-1

%A Bruce Perlmutter bruce@ispb.com
%A Jonathan Zarkower
%C One Lake St., Upper Saddle River, NJ 07458
%D 2000
%G 0-13-020335-1
%I Prentice Hall
%O +1-201-236-7139 fax: +1-201-236-7131
%P 268 p.
%T "Virtual Private Networking: A View From the Trenches"

The aim of the authors is to make this book different from others in the Virtual Private Network (VPN) field. In this they have, to a certain extent, succeeded. The book does not merely rehash old approaches, analogies, and illustrations. While this determined novelty does not always work, and sometimes gives the book a ragged feel, there is a

freshness to it that is engaging. Perlmutter and Zarkower also wanted to make the book fun: they don't always succeed, although their humour remains light throughout, and never descends into the heavy sarcasm that befalls most who insist on larding their books with jokes. The levity is amusing, but it isn't really illustrative.

The text also aims at a rather unique audience. As well as presenting the concepts to business people needing a basic understanding, the material emphasizes the ability of the Internet Service Provider (ISP), and particularly the small one, to offer VPN technology as a value added service. This means that the book looks at both sides of the picture, and the view thus generated is both interesting and useful.

Chapter one offers a good introduction to the basic concepts. The evolution of networking adds a depth of understanding to this prelude in chapter two. (I would note that the authors suggest cable modems and Digital Subscriber Line [DSL] technologies can be used in conjunction with VPNs in order to create a high speed connection between offices. It should be pointed out that both cable systems and the most common form of DSL have an inherent asymmetry of bandwidth that prevents this usage.) The business case for VPNs is made carefully and realistically in chapter three. Tunneling is discussed in chapter four, although some ends are left loose. An example of a problem with encapsulating Appletalk over PPTP (Point to Point Tunneling

Protocol) seems to beg the question of whether the application can be made to work. Chapter five is not simply a list of available products, but an outline of the types of VPN components and devices that can be used. Considerations to be made when choosing, and getting ready for, a VPN are brought forward in chapter six, while the ways that ISPs can offer service are examined in chapter seven. Chapter eight closes off with a realistic look at new technologies that will soon be affecting VPN decisions.

Within the book there are a number of boxed items. These are variously scenarios, sidebars, comments, or other material entirely, and it isn't always clear which they are intended to be. Many of the scenarios are extremely short, and really don't explain anything. These materials should not necessarily have been excluded, but more thought could have been given to their purpose, and whether or not they fulfilled it.

This is a practical and realistic guide to the reasons for, and construction of, a Virtual Private Network. Users (and particularly small to medium business users) and ISPs alike will benefit from the explanations herein.

copyright Robert M. Slade, 2000 BKVRPRNG.RVW 20000111
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

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

CFP: Safety & Reliability of embedded Software Systems

Pete Mellor <pm@csr.city.ac.uk>

Mon, 14 Feb 2000 17:34:09 GMT

SAFETY & RELIABILITY OF EMBEDDED SOFTWARE SYSTEMS
Special Issue of Quality and Reliability Engineering
International
(Issue 6, December 2000)
Wiley InterScience

CALL FOR PAPERS [abridged for RISKS. PGN]

This special issue will cover techniques for the development of dependable systems containing embedded software and the assessment of their levels of dependability.

Submission of abstracts:	31st March 2000
Submission of completed papers:	31st July 2000
Final versions of accepted papers:	15th September 2000

[Possible topics:]

- Techniques for fault avoidance: requirements capture, HCI design, formal specification methods, validation and verification.
- Techniques for fault removal: inspection, testing and system trial.
- Techniques for fault tolerance: redundancy, design diversity, ``belt and braces and a piece of string''.
- Techniques for dependability assessment: ``operational profile'' and definition of realistic operating environments for system trial, data collection, statistical analysis, quantitative demonstration of achieving targets, dependability apportionment, certification of dependability to conform to industrial or governmental standards.

[... For more info, contact]

Peter Mellor, Centre for Software Reliability,
City University, Northampton Square, London, EC1V 0HB
ENGLAND

Tel.: +44 (0)20 7477 8422

Fax.: +44 (0)20 7477 8585

E-mail: p.mellor@csr.city.ac.uk

The Wiley InterScience website is: www.interscience.wiley.com

Pete Mellor

USENIX Annual Technical Conference, 2000 - Preliminary Program

Moun Chau <moun@usenix.ORG>

Fri, 18 Feb 2000 11:53:45 -0800 (PST)

2000 USENIX Annual Technical Conference

June 18-23, 2000

San Diego Marriott Hotel & Marina

San Diego, California, USA

<http://www.usenix.org/events/usenix2000>

The USENIX Annual Technical Conference is the gathering place for like minds in the computer industry, a place to meet peers and experts and share solutions to common problems. Join us in San Diego on June 18 - 23, 2000 as we celebrate our 25th Anniversary and pave the way for future innovations.

* Keynote Presentation by Bill Joy, Co-Founder of Sun Microsystems

* Closing Presentation by Thomas Dolby Robertson, Founder of Beatnik, Inc.

* Refereed paper presentations and Invited talks includes new

work from

Bill Cheswick, Rob Pike, and Margo Seltzer; the latest research results

on operating systems, tools and techniques for dealing with the system

infrastructure headaches, and a discussion on the Microsoft Antitrust

Case by expert witness Edward Felten of Princeton University.

* The very popular Freenix track returns with topics on *BSD, Linux,

X11-based graphical user interfaces, and the full range of freely

redistributable software.

* BoFs and WiPs bring attendees together for informal reports on interesting new projects and on-going work. Fast paced and spontaneous,

WiPs and BoFs discuss new ideas and novel solutions. See website for

schedule and to reserve WiP slots.

For detailed technical and tutorial programs and online registration:

<http://www.usenix.org/events/usenix2000>

Sponsored by USENIX, the Advanced Computing Systems Association.

Information Survivability Workshop ISW 2000

Howard Lipson <hfl@cert.org>

Thu, 17 Feb 2000 02:12:12 -0500

October 24-26, 2000, Boston, Massachusetts USA (tentative)

Sponsored by the IEEE Computer Society

Organized by the CERT* Coordination Center, Software Engineering Institute

General Chair: Tom Longstaff, Technical Manager of R&D at the CERT/CC

ISW 2000 is the third in an ongoing series of IEEE-sponsored research

workshops in survivability. The Information Survivability Workshops provide a forum for researchers, practitioners, and sponsors to discuss the area of survivability, the nature of the unique (and sometimes not-so-unique) problems associated with survivability, and promising approaches to finding solutions to these problems.

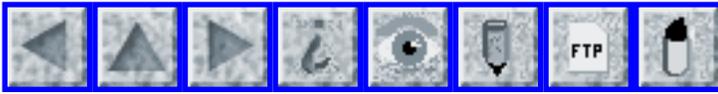
An emerging discipline, survivability extends the goals of traditional computer security to encompass concepts, methodologies, and tools that support the ability of a system to continue to fulfill its mission in the presence of attacks, accidents, and failures. The goal is not only to thwart attackers whenever possible, but also to build systems that are robust in the presence of attacks that cannot be completely repelled. [...]

The ISW 2000 call for papers will be distributed, within the next few weeks, to the same mailing lists as this announcement. The call for papers will also be posted at the ISW web site:

<http://www.cert.org/research/isw.html>

Proceedings from previous workshops (ISW'97 and ISW'98) are available at the same web site.

* CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 81

Monday 21 February 2000

Contents

- [Announcement of the ITS4 software security scanner](#)
[John Viega](#)
- [Hacker posts phony press release](#)
[Doneel Edelson](#)
- [Risks of untrusted provenance](#)
[Mich Kabay](#)
- [Senate web site dies, Clinton stresses Net-reliability](#)
[Declan McCullagh](#)
- [Windows 2000 leaves new court records system unreliable](#)
[Michael S. Keller](#)
- [Revenge of Authenticode](#)
[Mark Seecof](#)
- [Re: Distributed denial-of-service attacks](#)
[Giles D. Malet](#)
[Paul Oldham](#)
[William Colburn](#)
[Dick Mills](#)
- [Risks designed into the Internet](#)
[Charles J Wertz](#)
- [Michigan puts Doubleclick on notice](#)
[NewsScan](#)

- [Re: Microsoft responds](#)
[Tom Sheppard](#)
 - [Even more on risks with MS Outlook](#)
[John L Meissen](#)
 - [Two signatures](#)
[David E. Ross](#)
 - [Amazon password change practice](#)
[Thomas Roessler](#)
 - [Re: Risks of bouncing messages from closed e-mail lists](#)
[DeRobertis](#)
 - [Re: Risks of policies not thought out properly](#)
[Rumy Driver](#)
 - [Risks of mistaking a trademark for a generic word](#)
[Mich Kabay](#)
 - [A really clever privacy policy](#)
[Martin Minow](#)
 - [Re: Review of "Database Nation"](#)
[Dave Weingart](#)
 - [Info on RISKS \(comp.risks\)](#)
-

🔥 Announcement of the ITS4 software security scanner

John Viega <John@list.org>

Mon, 21 Feb 2000 10:35:00 -0800

[This is a nifty piece of work, and presents one more argument for

open-source software -- although I suppose proprietary software purveyors

might prefer to apply it themselves to closed-source systems! But it is

noteworthy that this analytic tool is itself open source. PGN]

I've put together a command-line tool for statically scanning C and C++

source code for security vulnerabilities. The tool is called ITS4. ITS4

scans through source code for potentially dangerous function calls that are stored in a database. Anything that is in the database gets flagged. ITS4 tries to automate a lot of the grepping usually done by hand when performing security audits.

The tool is available from: <http://www.rstcorp.com/its4/>
Also on this site is a research paper on ITS4 submitted to this year's Usenix Security conference.

ITS4 is open source software. The license puts some minor restrictions on commercial use. In essence, you can't use this tool to make money (such as by reselling it, or by using it in a consulting practice). However, you are encouraged to run the tool on your own product in order to make it better.

ITS4 does more than just grep-type work. It allows for arbitrary handlers to refine the initial analysis. This version of ITS4 comes with some simple handlers. Some of these handlers check for uses of common string operations that often are not significant problems. For example:

```
strcpy(buf, "\n");  
sprintf(buf, "%d", i);
```

In the first case, ITS4 will look at the second argument to a strcpy. If it is a string constant, the severity of the problem site is reduced to the lowest possible level. The tool will not output this kind of problem in its standard mode. In the second case, a similar reduction in severity occurs, since the sprintf format string contains no %s's.

The tool also has handlers that scan for file access race conditions, similar to the prototype tool discussed in [BD96]. We slightly improve on their tool by allowing for interprocedural and intermodular problems.

There are some technical limitations to this tool, many of which we hope to improve in the future. We'd like to have the help of the security community. I'm personally dedicated to improving this tool, and Reliable Software Technologies is willing to put some resources towards doing so. Changes from the community will certainly be considered for inclusion in future ITS4 releases.

Currently, the weakest area of ITS4, where the input of the security community is most important, is the vulnerability database, which was largely taken from some very preliminary work done by Tom O'Connor. It's perhaps a good start, but far from complete. Many new things could be added, and the entries that do exist can likely be improved substantially. For each database entry, we have a description, a default severity, and a recommended alternative. Generally, the descriptions are pretty scant, and the severities are not overly well thought out.

The next area for improvement is the handlers. It would be great to see people writing some good handlers, or even suggesting good handlers, and then we could write them.

Beyond that we're interested in the following:

- 1) Flagging the allocation mechanism used on important variables (i.e., stack-allocated buffers are usually easier to exploit than heap-allocated buffers if there is an overflow).
- 2) Performing much better static analysis. We'd probably like to start by building some sort of heuristic alias analysis, and then doing something similar to the analysis done in [WF+00].

We do have plans to ultimately do these things, but if other people want to code them up and contribute to the project, that's great.

I've set up a mailing list for people who are interested in helping out in any capacity. Hopefully we can get a good discussion going that will improve the vulnerability database, and make ITS4 a far more useful tool.

The mailing list signup is available at:
<http://www.list.org/mailman/listinfo/its4>.

John Viega, Software Security Group Co-founder
Reliable Software Technologies
viega@rstcorp.com

References:

[BD96] M. Bishop and M. Dilger. Checking for race conditions in file accesses. *Computing Systems*, 9(2):131-152, Spring 1996.

[WF+00] D. Wagner, J. Foster, E. Brewer, and A. Aiken. A first step towards automated detection of buffer overrun vulnerabilities. In *Proceedings of the Year 2000 Network and Distributed System Security Symposium (NDSS)*, pages 3-17, San Diego, CA, 2000.

⚡ Hacker posts phony press release

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

Thu, 17 Feb 2000 18:57:26 -0500

A fake press release announced a merger of Aastrom Biosciences Inc. with Geron Inc., a California biopharmaceutical house. Aastrom stock fell, while Geron rose. Aastrom asserted that the message on their Website was totally bogus, and presumably the result of a penetration. [Source: United Press International - 17 Feb 2000; PGN-ed]

⚡ Risks of untrusted provenance

Mich Kabay <mkabay@compuserve.com>

Fri, 18 Feb 2000 10:12:08 -0500

According to a 17 Feb 2000 AP item (18 Feb 2000 article in *The Washington Post* by David Ignatius, the US State Department has its shorts in a knot because they have just realized that a software package called the Mission Performance Plan that is running on embassy computers around the world was written by programmers from the former Soviet Union. On 2 Feb 2000, the Department of State sent an urgent cable to 170 embassies ordering them to remove the package by the 7th while security specialists examine the code for trap doors, logic bombs and other cybernasties.

[Comment by MK: this incident reinforces the view that the trustability of

software writers is even more important than quality assurance where security is concerned. As many commentators have noted, it may be impossible in practice to apply adequate quality assurance to untrusted code. I have frequently urged QA specialists to ensure that they use code-coverage logging to ensure that every line of code is actually executed during the SQA process; however, even total coverage does not necessarily mean that a program is guaranteed safe, since variable sequence of execution could result in different outcomes for the same subroutines because of data dependencies.]

M. E. Kabay, PhD, CISSP / Security Leader, INFOSEC Group / Adario, Inc.

⚡ Senate web site dies, Clinton stresses Net-reliability

Declan McCullagh <declan@well.com>

Tue, 15 Feb 2000 21:05:27 -0500

<http://www.wired.com/news/politics/0,1283,34362,00.html>

The Crash of a Dot.Gov, by Declan McCullagh (declan@wired.com)

Wired, 15 Feb 2000

As government aides were frantically preparing for the president's last-minute Internet-reliability summit with technology leaders, thousands of visitors couldn't reach the U.S. Senate's own Web site. It was offline for over nine hours Monday, from early afternoon to after 11 p.

m. (EST) due to technical problems, Senate officials said. The embarrassing site failure comes just as the U.S. government is telling private firms how important it is that they increase the reliability and security of their own networks.

"Our administration has been working for years now to reduce vulnerabilities in government computers and to encourage the private sector to do more,"

President Clinton said before Tuesday's one-hour meeting with corporate information officers, academics, and Cabinet members.

From Declan's POLITECH, a 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/>

⚡ Windows 2000 leaves new court records system unreliable

"Michael S. Keller" <mkeller@mail.wcg.net>

Mon, 21 Feb 2000 14:07:51 -0600

The full article resides at

<http://search.tulsaworld.com/archivesearch/default.asp>

?WCI=DisplayStory&ID=000219_Ne_a10court

<A

HREF="[http://search.tulsaworld.com/archivesearch/default.asp?](http://search.tulsaworld.com/archivesearch/default.asp?WCI=DisplayStory&ID=000219_Ne_a10court)

[WCI=DisplayStory&ID=000219_Ne_a10court](http://search.tulsaworld.com/archivesearch/default.asp?WCI=DisplayStory&ID=000219_Ne_a10court)">

A new state-run computer system for the Tulsa County Court Clerk's Office

that was supposed to be the envy of the rest of the country is still

malfunctioning, sometimes for days on end. The new system was

put in place
just a few days before the end of 1999 in an effort to make the
court
records system Y2K compliant. Still, (Sally) Howe Smith said,
the old days
under the clunky mainframe are starting to look pretty good.
The new system
has been down completely for at least a day twice in the last
two weeks and
regularly has system errors that hinder access to records for
hours at a
time, she said. The court records system uses Windows 2000, and
the new
software was deployed early for the state system. (Website
coordinator
Gregg) Lambert said state technicians were hoping to confer with
Microsoft
officials about some of the system's problems.

Michael S. Keller, Technical Solutions Consultant,
Sprint Enterprise Network Services, Amateur Radio N5RDV

🔥 **Revenge of Authenticode (Re: [RISKS-18.89](#))**

<msecof@seatimes.com>

Fri, 18 Feb 2000 09:59:43 -0800

Microsoft (hereinafter MS) Windows 2000 has a kind of "immune
system"
feature which causes it to reject any driver or DLL update which
has not
been digitally signed by Microsoft. The signature system looks
to be
similar to Authenticode.

In [RISKS-18.89](#), I suggested that the real utility of MS'
Authenticode was to
assist MS marketing. I offered a test for my hypothesis: that
an offer by

MS to sign others' code (for a fee) would validate my theory.

Well, if you want to supply a new device driver (say, for a variant peripheral) or library update (adding, say, some spiffy cryptographic features) for Windows 2000, you must give your code to MS for early review and pay MS a fee. If you do these things, MS may sign your software. If you do not, then no Windows 2000 machine will run your code (or at least, not without big trouble, too big for non-techies).

As with Authenticode, MS' scheme is not unbreakable, nor does it even attempt to assure the quality (as opposed to the provenance) of signed code. (Oh, MS says their lab will review 3rd-party code for "compatibility," but they won't check for malware, and unlike, say, Java's sandbox, MS signature scheme has no inherent malware-inhibiting qualities).

MS marketing will stop at nothing, Q.E.D..

Mark Seecof

✶ Re: Distributed denial-of-service attacks (Cox, [RISKS-20.79](#))

Giles D. Malet - IST <gdmalet@ist.uwaterloo.ca>
21 Feb 2000 10:16:53 -0500

> ...pronounce "DoS" to rhyme with "sauce" -- and sound just like "DOS".

For those of us that don't speak American that sentence makes no sense at all. The pronunciation of "DOS" comes nowhere near that of

"sauce". In English, they rhyme more with "moss" and "morse" (with a silent `r`) respectively. Risky assumptions about your readership?

[Webster of course gives a British spin on "doss" --
1. doss \'da:s\ vi [origin unknown] chiefly Brit :
to sleep or bed down in any convenient place
2. doss n chiefly Brit : a crude or makeshift bed
Dictionaries and linguistic differences make strange
bedfellows.

I presume the OED doss even better. But phonetically auf deutsch, we have

"Dos ist gut, net?" (where "net" is regional dialect for "nicht"). PGN]

🔥 Re: Distributed denial-of-service attacks (Cox, [RISKS-20.79](#))

Paul Oldham <paul@the-hug.org>

Mon, 21 Feb 2000 15:55 +0000 (GMT Standard Time)

You say "tomato"?

> I heard more than one reader pronounce "DoS" to rhyme with "sauce" [...]

It took a few seconds for me make any sense at all of his comment: when did "DOS" ever rhyme with "sauce"?! And then I realised that Ken is probably an American-English speaker and that he had missed another risk: that all readers of english will pronounce words the same way.

Let's call the whole thing off.

Paul Oldham, Milton, Cambridge, England

<http://the-hug.org/paul/>

⚡ Re: Distributed denial-of-service attacks (Cox, [RISKS-20.79](#))

"Schlake (William Colburn)" <schlake@nmt.edu>
Mon, 21 Feb 2000 08:10:30 -0700

It could easily be argued that DOS is a DoS against the Intel processor family.

⚡ Re: Distributed denial-of-service attacks (Cox, [RISKS-20.79](#))

Dick Mills <dmills@IASystems.com>
Mon, 21 Feb 2000 08:44:02 -0500

This reminds me of a counter example.

Three or four years ago the following joke made the rounds.

"What do you get if you cross Lee Iacocca with a vampire?

AUTOEXEC.BAT"

I was astounded at how many people got it. Even technophobes and Mac owners understood it and laughed. Maybe Murray Hill NJ would be the only place on earth that it would flop. :)

My point is that these things are less jargon-like than we might think.

They are at least slang and perhaps mainstream American English by now.

⚡ Risks designed into the Internet

Charles J Wertz <wertzcj@buffalostate.edu>

Sat, 12 Feb 2000 12:18:15 -0500

The recent flurry of discussions and warnings about cross site scripting is but one more reminder of the vulnerabilities that result from the basic design (?) of the internet, http, scripting languages, and most browsers.

Meanwhile, we find that more and more sites refuse to function unless javascript and/or cookies are enabled. Some warn us of this. Some, www.anybirthday.com for example, just give misleading results. And of course, some Microsoft sites demand Internet Explorer with vbscript turned on.

There seems to be a clear cut choice between "safe browsing" and access to a lot of the information that is available on the web. Web sites could be designed to work acceptably without client side scripting, but it is unlikely that many folks will decide to do so.

So, I guess I'm just complaining. Does anyone have a better idea?

⚡ Michigan puts Doubleclick on notice

"NewsScan" <newsscan@newsscan.com>

Fri, 18 Feb 2000 09:44:23 -0700

The attorney general of Michigan has filed a "notice of intended action"

against DoubleClick, charging the Web advertising firm with "failing to disclose to Internet users that DoubleClick is systematically implanting electronic 'cookies,' or electronic surveillance files, on hard drives of users' computers without their knowledge or consent." In addition, the notice criticizes DoubleClick's recent attempts to combine its tracking data with personal data such as names obtained through its acquisition of Abacus Direct last year. Michigan's filing, which is preliminary to a lawsuit, is the third action taken against DoubleClick this week -- the Federal Trade Commission and the New York attorney general earlier launched separate inquiries into the company's business practices. [*Financial Times*, 18 Feb 2000, <http://www.ft.com/>; NewsScan Daily, 18 Feb 2000]

⚡ Re: Microsoft responds (Allchin, [RISKS-20.80](#))

Tom Sheppard <TSheppard@home.com>
Mon, 21 Feb 2000 12:41:26 -0500

I find Jim Alchin's rebuttal in [RISKS-20.80](#) dispelling the rumour of 63,000 defects in Windows 2000 hilarious.

This statement got me laughing out loud, "We also have a special advanced source code analyzer that we use. This tool generates a significant number of false positives (it thinks the code should be changed, but in fact it should not be)."

This "advanced" analyzer generates "significant" false positives. I guess it must be as advanced as Windows 2000. So how many defects are logged against the analyzer, Jim?

Mr. Alchin goes on to state, "We love this tool."

And we all love Windows, Jim. Truly we do.

...Tom

✦ Even more on risks with MS Outlook (Clemson, [RISKS-20.79](#))

"Meissen, John L" <john.l.meissen@intel.com>

Wed, 16 Feb 2000 10:38:30 -0800

> The bug is with pine -- it returns multipart/alternative and
> should have returned multipart/mixed. [...]

This is the sort of "force the user to adapt to the software instead of vice-versa" attitude that seems to permeate PC software. I find it incredibly frustrating that I'm constantly fighting software because someone assumes their way is the ONLY way something should be done.

Just because the client is HTML-aware doesn't mean it should hide the alternatives from you. My personal choice for e-mail (not what I'm forced to use at work) tells me there are alternate views available and lets me choose which one I would like to view. Sometimes I get e-mail which is all HTML. Having an HTML-aware client is handy in these cases. However, I don't like HTML, I don't want HTML, and given a choice I will view as

non-HTML. A product which forces HTML on me is broken, IMHO.

I agree that in this case there is a problem with Pine. However, while Outlook may be working as designed I would certainly argue that it is not working as it should!

⚡ Two signatures

"David E. Ross" <rossde@acm.org>
Sun, 20 Feb 2000 15:18:11 -0800

The situation:

Because of high-speed processing of bank checks without any human intervention, banks (at least in California) will no longer honor requests by depositors that checks have two signatures. Even when a check has imprinted on it "Two Signatures Required", banks will honor that check with only one signature.

When establishing a new account or when changing signature authorizations on existing accounts, banks are requiring depositors to sign a waiver that releases the bank from any liability for paying a check with only one signature. As long as the signature is in the bank's files, the loss will then fall on the depositor even if the signature card in the files or the check clearly indicates "Two Signatures Required".

The risk:

This can be a problem for non-profit organizations, many of

which depend on amateur help -- unpaid volunteers -- to handle administrative tasks, including disbursing funds. The California Attorney General -- who regulates charities through the state's Registry of Charitable Trusts -- recognizes the risk of embezzlement or other losses and strongly urges all non-profits to require two signatures on all checks. The use of a single authorized signature on a check has already proven insufficient. Losses to PTAs, high school booster clubs, and other volunteer-run non-profits are far too common.

Of course, businesses and other organizations are also at risk of loss without the safeguard of requiring two individuals to approve payments of funds. For that reason, a company's independent auditors will often require the use of two signatures if they are to certify the adequacy of the company's internal fiscal controls.

Some questions:

Automated pattern-recognition capabilities might not be sufficient to verify check signatures. However, the technology has surely advanced to the point where at least the presence of two signatures could be verified. It certainly can detect a preprinted "Two Signatures Required" on a check. Why have the banks not incorporated this technology into their check-clearing systems?

The banks claim they cannot stop the automated processing of checks and

examine each check to ensure that it has the correct number of signatures.
That is why they do not want to be held liable when a check marked "Two Signatures Required" is honored with only one signature. However, they also cannot stop the automated processing of checks and examine each check to ensure that it has a valid, authorized signature. Yet they remain liable if a check with an invalid signature is paid. What is the difference?

David E. Ross <<http://www.vcnet.com/~rossde/>>.

✶ Amazon password change practice

Thomas Roessler <roessler@guug.de>

Mon, 21 Feb 2000 13:18:58 +0100

Amazon.de has a very simple scheme for changing your account's password in case you forget it: Just tell their server your e-mail address, the title or ISBN number of a book you have ordered with them, and the last five digits of a bank account or credit card number you have used to pay. The server will happily permit you to change your password.

The RISK? The information to be supplied may be easily guessed.

Bank account numbers are readily accessible to - almost - the public; it's even common to put them onto letterheads. As opposed to credit card numbers, they aren't treated as secrets. Guessing what books have been ordered can frequently be easy, too - people tell about books,

people write reviews, or you just know peoples' interests. Trying best-sellers will work nicely as a large-scale attack.

The one and only element of control you have is a confirmation message sent to your e-mail address. While this may work if you are reading your e-mail regularly, a prolonged week-end vacation may be sufficient for an attacker to order a book, get it paid with your credit card (or from your bank account), and get it delivered to some empty building.

⚡ Re: Risks of bouncing messages from closed e-mail lists **(RISKS-20.79)**

"DeRobertis" <derobert@erols.com>
Thu, 17 Feb 2000 01:12:26 -0500

>However, there is a more serious vulnerability here: infinite loops between
>two or more closed lists. [Kabay]

Bounces should honor the Received: line count and add an extra one. Not only does this prevent infinite loops, but it also makes spam more trackable.

I'd think many already do something to prevent infinite looping; otherwise what happens if a from address is invalid? Bounce bounce bounce... until some sysadmin stops the flood?

✶ Re: Risks of policies not thought out properly

Rumy Driver <rdriver@sybase.com>

Mon, 21 Feb 2000 08:33:18 -0600

I have to fly to California for training. As my wife has never been to CA, I did book her ticket on American Airlines (My company has an agreement with them).

When I called after a couple of days to ask why I did not get a confirmation in the mail, I was informed that my credit-card processing was not complete as they had incorrect information about my ZIP code. I did ask as to why I was not informed and they said they di try to do so - by sending me a post card!!! YES, that's right - to inform me that they had an incorrect address on file they "mail" a post card.

I did speak to a supervisor who informed that "this is the official policy". I did ask him how this could be implemented and how it would work - "this is official policy".

The only way to inform Customer Relations is to call or send mail via the USPS. They do not have an e-mail address.

American Airlines
Customer Relations MD 2400
P.O. Box 619612
DFW TX 75261
(817)967-2000

Rumy Driver, Sybase Technical Support

[By all means, write them and complain! PGN]

⚡ Risks of mistaking a trademark for a generic word

Mich Kabay <mkabay@compuserve.com>

Thu, 17 Feb 2000 17:04:49 -0500

In connection with an item posted recently in RISKS on using automated rejection messages as a spam relay, I received the following correction from a list manager who asked to remain anonymous:

> Therefore I recommend that at the very least, administrators
> for closed e-mail lists prevent their listserv from sending ...

LISTSERV is a registered trademark of L-Soft International.
See:

<http://www.l-soft.com/>

Unfortunately, like "Kleenex" and "Rollerblades", "LISTSERV" has come to be commonly used to refer to any mailing list management package (or worse, the mailing list itself). Please pardon this one-man campaign to try and stop this practice. :-)

I responded that I would henceforth use the phrase "list-server software."

M. E. Kabay, PhD, CISSP / Security Leader
INFOSEC Group / Adario, Inc.

[RISKS has been doing so for a long time. PGN]

⚡ A really clever privacy policy

Martin Minow <minow@pobox.com>

Fri, 11 Feb 2000 23:31:36 -0800

Try reading the privacy policy of <<http://www.foxkids.com>> using Internet

Explorer 4.5 on the Macintosh. Be sure to use a color monitor and enable the "allow page to specify fonts and colors" option. You will see tiny black text on a dark blue image background: i.e., essentially unreadable.

If you turn off "show images," you get black text on a black background.

On Netscape Communicator, you get white text on the blue image, which is readable, even though the size "0" text is tough going without a magnifying glass. It's about 8 pt on my display.

The problem is that the page explicitly sets the page background color to "black" but does not set the default text color. The heading text "by using this site, you agree to the privacy policy of FK [Fox Kids] ..." is rendered in a HTML table element whose font is explicitly set "white", but the rest of the page, containing the policy itself, lacks an explicit font color. Netscape apparently continues to use the current font and text color until changed, while Internet Explorer reverts to the default color when the table element completes.

The entire privacy document is over 3,000 words long, but that's another story.

Martin Minow <minow@pobox.com>

[Well, it is not a *short* story, but in 8-point type
it's certainly a space saver rather than an eye saver!
The art of fine print strikes again. PGN]

⚡ Re: Review of "Database Nation" (Spafford, [RISKS-20.79](#))

Dave Weingart <dweingart@chi.com>

Wed, 16 Feb 2000 09:00:51 -0500

>... Simson recounts that people are able to get their credit
records or
>medical records from MIB, but then doesn't provide any
information on how to
>get them or who to contact; ...

That's because anyone who is contacted by MIB gets a little
light flashed
in their eyes and forgets all about it.

Dave Weingart, Randstad North America dweingart@chi.com 1-516-
682-1470



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 82

Monday 28 February 2000

Contents

- [U.S. government abandons Bernstein restrictions](#)
[Jeremy Epstein](#)
- [How to make friends, influence hackers, and build bugfree code Paris style](#)
[Peter Wayner](#)
- [Someone making sense about e-commerce](#)
[Paul Robinson](#)
- [The Millennium Bug Revisited](#)
[R A Downes](#)
- [It was just a network board...](#)
[Debora Weber-Wulff](#)
- [Risks of National Weather Service tests](#)
[John O Long](#)
- [Re: Microsoft responds](#)
[R A Downes](#)
- [Re: Great West gives out too much personal info](#)
[Taylor Hutt](#)
[Bob Hofkin](#)
- [Imbalanced parentheses or angle brackets](#)
[W.T. Shymanski](#)
- ["Unstable" postal addresses](#)

[Joseph A. Dellinger](#)

● [REVIEW: "Security Technologies for the World Wide Web", Rolf Oppliger](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

✂ U.S. government abandons Bernstein restrictions

Jeremy Epstein <jepstein@monumental.com>

Thu, 24 Feb 2000 17:04:37 -0500 (EST)

In light of the new export restrictions, the Commerce Department has abandoned all claims that Prof. Daniel Bernstein is restricted in posting his Snuffle encryption source code to his web site, according to a Reuters article at <http://www.wired.com/news/politics/0,1283,34550,00.html> .

However, the article says "'We are still considering our options,' said Cindy Cohn, Bernstein's lawyer. Cohn said the Commerce Department letter failed to clear up some questions about the new rules." [See PGN note below.]

--Jeremy

[The *Wall Street Journal* 25 Feb 2000 noted that the residual questions are on areas of ambiguity such as mirror sites and a restriction on access in countries suspected of supporting terrorism. PGN <http://interactive.wsj.com/articles/SB951422940442620073.htm>]

✂ How to make friends, influence hackers, and build bugfree code Paris style

Peter Wayner <pcw@flyzone.com>

Sat, 26 Feb 2000 10:36:22 -0500

The **Times** (London) reported on 26 Feb 2000 that Serge Humpich, a hacker, was convicted of fraud and given a suspended sentence. The young man discovered how to trick the Carte Bleue system and claimed he could have gone on an unlimited spending spree. Instead he hired lawyers and negotiated with the company that runs the system for payment in return for detailing the problems. The company turned around and prosecuted him for fraud after they arranged for him to demonstrate the system.

What a brilliant way to discourage folks from rooting around in a system and reporting security flaws! I wouldn't be surprised if their system proves to be so impervious that the number of bug reports drop to zero. What a wonderful solution for creating bugfree code!

⚡ Someone making sense about e-commerce

Paul Robinson <Rfc1394a@aol.com>

Wed, 23 Feb 2000 08:45:03 EST

When we think about the risks of technology, we often think about the risks to life and property. But the risks of technology are caused because people don't think about the possible consequences of relying on technology. Sometimes it does good but if you don't know when technology isn't the

solution you're taking a big risk.

In the following link, the CEO of Liz Claiborne, Paul Charron, explains why he's not jumping whole hog into Internet sales. It's a breath of fresh air in the otherwise rarefied atmosphere of the e-commerce market to hear from someone who has seriously thought about what he's doing:
<http://www.computerworld.com/home/print.nsf/CWFlash/000221EDB2>

It shows that he understands the risks of trying to spend several million dollars on setting up a web site to sell something when it might not create profitable returns for 20 years or might merely cannibalize brick-and-mortar sales. If a few more people had thought about this, maybe we wouldn't have an Amazon.Com and 200,000,000,000,000 other on-line commerce sites losing tens of millions of dollars every year. Okay, so I'm exaggerating (but not by much).

Has anyone ever thought about the fact that in general, the only web sites that are consistently making money are the ones dealing in pornography? This brings new meaning to the term, "obscene profits". :)

Paul Robinson <postmaster@paul.washington.dc.us><A
HREF="<http://paul.washington.dc.us>"> <http://paul.washington.dc.us>
us

The Millennium Bug Revisited

<main@radsoft.net>

Wed, 23 Feb 2000 20:46:11 +0000

Y2K is here and on a roll: things went better than expected; Clinton's administration is declaring a total victory. The real Millennium Bug - Windows 2000 - has had much worse luck. Further, it is now apparent that there are two such bugs: the operating system itself, and the hype campaign now introduced to get us all to once again jump on the merry bandwagon of planned obsolescence and upgrade to it.

None other than Paul Thurrott of Windows NT Magazine has declared, after admitting that a lot of Win2K, such as tooltips that not only "display" as before, but now "roll in" and "roll out", is "fluff" and no more, that these supposed enhancements are "good for the end user". It remains a mystery, however, to both the undersigned and many more, how a rolling tooltip can be regarded as a substantial end user improvement.

Sanity. Keeping a level mind. Let's remember that the shortest distance between two points in this case, the distance between what a user wants and what the operating system does to the hardware, has not increased by one iota. File operations are still file operations (encryption on disk an option and not a requirement); video RAM updates are identical; everything in fact is the same. There is no reason whatsoever for any of these basic operating system functions to require more hardware - CPU speed, disk space, RAM - to work. There is no reason for the operating system to exhibit the extreme sluggishness it does.

"When things get too slow, we just throw more hardware at it."

This, the
"Rule of Redmond", obvious everywhere in Redmond code, is
especially
prevalent in the code of Windows 2000. And while it is an
affront to our
collective human intelligence to expect to be able to sell us on
the
assumption that the same operations which ran so fast on previous
versions can suddenly run so agonizingly slow with even twice or
four
times the processing power on this one, it is not without our
collective
human imagination to understand - or even predict - why and how
this
"fluff" - this junk - can have that effect.

When things deteriorate to the point where a major Internet
authority
slips into saying that rolling tooltips make matters better for
an end
user, then we know we have been hit - by the second of the lethal
Millennium bugs.

Windows 2000 has not at all received the welcome Redmond would
want.
Long before its release the Microsoft Windows 2000 Redeployment
Program
fell completely apart. ISVs and OEMs and major corporations
everywhere,
after seeing the frightening wave of the future with the betas,
decided
to jump ship. Polls conducted as recently as days before the
official
release of Windows 2000 indicate most of these same corporations
naturally have no inclination whatsoever to upgrade to Win2K and
even
less inclination to take it into consideration when writing new
software. So Microsoft has been hard put. And, to make matters
worse for
them, a Finn has entered their arena, becoming a nemesis that
they fear
more than we can ever really appreciate. Microsoft is not making
inroads

in the net server market, and this must hit them hard too, as do relations with the DOJ in Washington. So under the circumstances, watching Microsoft do its little propaganda dance, and now do it a bit more openly and a bit more brazenly than in the past, makes an interesting study indeed.

Maybe we didn't really notice last time around - if you reckon the inception of Windows 95 as "last time" - the kind of hype we do today. Maybe it was there and we just didn't notice it. But today, most likely because of the circumstances, it seems to stand out more:

- We're told that this is the best product Microsoft has ever released (there's a noticeable echo on this one: we've heard it before, and been gravely disappointed before too - what else can we expect them to say).

- We hear things like "we really love this product". Over and over again. The power of suggestion, of repeating the "big lie", has become a weapon in the Redmond camp.

- We're told Win2K runs faster than both 95 and NT 4 on the kind of hardware running 95 and NT 4 today, when we've all seen that the contrary is true.

- Supposedly independent computer science authorities are heard to mumble incredible things such as those mentioned above. (Another gem came about in the wake of the rumour that Win2K has over 60,000 bugs: suddenly these "authorities" are claiming that none of these bugs will ever be noticeable by end users).

We know that not all these dupes are on the Microsoft payroll. We don't assume, to paraphrase Lyndon B. Johnson, that Microsoft has everyone's CPU in their pocket. But we do see that the cult of mania begun by Microsoft with the release of Windows 2000 is spreading, and that many individuals who normally consider themselves sane and level headed are unwittingly acting as dupes of the International Microsoft Conspiracy of planned obsolescence.

This seems somewhat borne out by the fact that Microsoft even attempted to keep good old NT 4 away from ISVs involved in their development network (MSDN). It is borne out by the fact that several key NT applications (such as File Manager) have been deliberately sabotaged by the Win2K team. And further evidence of Microsoft's desperation might be upon us before this letter is even sent.

Let's get this absolutely straight: no one "needs" Win2K. There is nothing inherent in Win2K that we have been desperately longing for. No advocate of Win2K can come with a long and impressive list of enhancements that have been conspicuous in their absence from Windows NT. All we really know is that Microsoft has decided, as so often in the past, that it is time again for their "out with the old and in with the new" marketing coup. Even Intel's claims that Win2K is horrendously slow, so slow that they themselves need to invest in new hardware for \$50 million, must be taken with a grain of salt. There is no way Microsoft will ever tell us the truth: they were

not going to admit that Windows 95 was a RAM hog and needed four times the CPU speed and RAM as its predecessor, and they are not going to admit that Windows 2000 doubles even that multiplication figure. No, they are going to let us figure this all out by ourselves: the more processors they can help Intel and others sell the better. Look at Michael Dell: in one breath he fells a comment about Windows 2000 which sends Microsoft stock plummeting; in the next he tells of his decision to run his web site with it.

So there's a second bug here all right, almost more dangerous than the first and a lot more contagious. And there are no known vaccination serums available.

RA Downes Radsoft Laboratories <http://www.radsoft.net>

⚡ It was just a network board... (Re: [RISKS-20.75](#))

Debora Weber-Wulff <weberwu@tfh-berlin.de>

Mon, 28 Feb 2000 13:15:52 +0100

The Berlin Fire Department has found the culprit! RISKS readers recall the problems the Berlin Fire Department had starting 4 minutes after midnight on 1 Jan 2000: The dispatching system went awry, believing that fire trucks were in places they weren't, dropping emergency calls on the floor, confirming dispatches that never were forwarded, etc, etc.

In anticipation of Leap Day they have been busy testing and testing the

system. Lo and behold, they can repeat the behavior for 29 Feb 2000. It turns out that a handful of network cards, costing about \$50 a piece, were not able to handle either date, and were generating erratic packets.

Replacing the boards has fixed the problem, according to *Der Tagesspiegel*.

[<http://www.tagesspiegel.de/archiv/2000/02/24/ak-be-st-32899.html>]

The police union criticizes that this system behavior had been observed before, but no one ever bothered to find the source of the problem. The police ended up fighting fires with water cannons instead of the fire department using all those shiny new fire engines they bought from a German automotive company after the fire chief was lent a nice car from the same company.

Prof. Dr. Debora Weber-Wulff, Technische Fachhochschule Berlin
weberwu@tfh-berlin.de, <http://www.tfh-berlin.de/~weberwu/>

Risks of National Weather Service tests

<jllong@us.ibm.com>

Mon, 28 Feb 2000 13:12:33 -0500

Today, I was checking the weather on the MyYahoo web page I have created. I noticed that there was a red asterisk by the listing for the city I live in.

The red asterisk is denoted as meaning "severe weather alert". This was strange, since the forecast summary showed a sun, indicating a clear, sunny

day. I clicked to get the full weather report, which indicated a normal sunny day, but a clickable line that said "severe weather alert". I clicked on the severe weather alert to find the following:

ALAMANCE, ANSON, CHATHAM, CUMBERLAND, DAVIDSON, DURHAM, EDGECOMBE, FORSYTH, FRANKLIN, GRANVILLE, GUILFORD, HALIFAX, HARNETT, HOKE, JOHNSTON, LEE, MONTGOMERY, MOORE, NASH, ORANGE, PERSON, RANDOLPH, RICHMOND, SAMPSON, SCOTLAND, STANLEY, VANCE, WAKE, WARREN, WAYNE, WILSON, INCLUDING THE CITIES OF BURLINGTON, CHAPEL HILL, DURHAM, FAYETTEVILLE, GOLDSBORO, GREENSBORO, RALEIGH, ROCKY MOUNT,

925 AM EST MON FEB 28 2000

...FROM THE NATIONAL WEATHER SERVICE...THIS IS A TEST HIGH WIND WARNING ONLY... THIS IS ONLY A TEST.

It would appear that the text scanner that looks for severe weather announcements is unable to determine when it's only a test.

The risk is probably very small. However, as more and more people rely on automated reporting data from various sources, we will find that many of these sources were not really created for direct pass-through of information. Direct, live testing of systems such as the National Weather Service is important, but unless this is carefully handled by vendors on the web, we could have a lot more miscues sent to the general public.

John O Long/Raleigh/IBM@IBMUS, jllong@us.ibm.com
Programming Consultant, Solution Architecture and Reuse
919.993.4208

✉ Re: Microsoft responds (Allchin, [RISKS-20.80](#))

<main@radsoft.net>

Tue, 22 Feb 2000 01:20:08 +0000

Tom Sheppard <TSheppard@home.com> writes of a possible 63,000 bugs in Win2K. Tom is still the Titanic in search for the tip of an iceberg.

The internal rule in Redmond is "4 bugs per KLoC".

Ok. A KLoC is 1000 (or 1,024) lines of code.

Windows NT was only 16 million lines of code. Piece of cake.

But Windows 2000 - without the likes of Cutler, without being a direct copy of VMS and Prism - is four times that size. Written by people with a fraction of the talent.

We're talking about 50,000 or 60,000 KLoCS. Microsoft themselves say 4 bugs per KLoC. Go figure.

...and I think we must remember that we can never have a debate on the merits or shortcomings of Windows 2000. On the one side we have inquisitive minds authentically attempting to arrive at the truth, on the other we have the clever minds of those like Alchin who are simply trying to sell a product by any means. Windows 2000 will always be the best and most stable and fastest and most loved product ever. It will run faster on a Z80 than CP/M. We will always really love this product.

⚡ Re: Great West gives out too much personal info (Hutt, [RISKS-20.80](#))

Taylor Hutt <t.hutt@worldnet.att.net>

Fri, 25 Feb 2000 06:24:52 GMT

Last week I submitted a message about Great West giving away too much information (Name, birthdate, SSN, account number) in a confirmation letter regarding a change-of-address.

I spoke to the person in charge of the account (Nancy Lynch) and she indicated that a meeting with management was to be held this week; she would raise the issues and get back to me.

Well, I'm here to report that she did get back to me and has informed me that Great West will not be putting the SSN of a person on any correspondence effective immediately. Further, they will be doing a systematic review of all correspondence to determine which information is actually pertinent to that correspondence. (She even offered to keep me up-to-date with their progress on that, but I told her I didn't think that would be necessary)

I am pleased at the speed which Great West has addressed this situation and am once again invigorated to believe that it is possible to change the system.

Hats off to Nancy for carrying through so well on this one.

Taylor Hutt

✈ **Re: Great West gives out too much personal info (Hutt, [RISKS-20.80](#))**

Bob Hofkin <bhofkin@erols.com>

Sun, 27 Feb 2000 14:46:40 -0500

Taylor Hutt wrote about his 401(k) company mailing out all of his account identifying information in one letter.

I had a similar problem with Cigna a couple of years ago. They convinced our HR Person to have them send out letters with lots of personal identifying information, and a pitch to sign up for their on-line service, Neither the HR Person nor any of the Cigna reps I spoke with seemed to understand that anyone who intercepted the letter could commandeer my account. Cigna claimed the system met their internal security guidelines(!!) and besides, even if something did go wrong, I would see it on my quarterly statement and they would be happy to fix any problems. I can just imagine the phone rep: "Sure thing, we'll be happy to move that \$100,000 right out of the fund that lost 2% and back into the one that made 24%, and of course we'll make that retroactive. So sorry to inconvenience you in the least."

Perhaps this is standard procedure in the industry. I was surprised at the lack of security awareness and the lack of concern. One comment

that was no
surprise: "You're the first person who ever complained about
this."

✂ Imbalanced parentheses or angle brackets

"W. T. Shymanski" <"nski\" <nski\" <nski\" <nsk"@mts.net>
Mon, 21 Feb 2000 19:29:27 -0500

I had the misfortune last week to photocopy a customer request
for proposal
document that I needed to work with. While frantically trying
to put the
proposal out before the deadline, I noticed the requirements
seemed a little
sketchy in parts; examination of two pages showed that the set
of points was
numbered 1,2...big white space at bottom of the page...5,6 on
the next page.

It turned out that our digital Pitney-Bowes photocopier had
developed a
problem where it would not print the bottom half of a page. For
spreadsheet
pages printed in landscape format the error was quite prominent,
since the
left-hand-side of the page was blank. But for regular portrait-
mode text,
it was only because the following page had paragraphs numbered
out of
sequence that I even noticed the problem.

The risks are pretty obvious: potentially the difference between
profit and
loss on any given contract might hinge on a paragraph at the
bottom of a
page, which the digital photocopier might softly and silently
eat without
trace. Normal analog-type photocopiers in my experience don't
make *this*

type of foul-up.

Bill Shymanski <wtshyman@mb.sympatico.ca>

✶ "Unstable" postal addresses

"Joseph A. Dellinger" <jdellinger@amoco.com>

Mon, 21 Feb 2000 20:46:49 -0600 (CST)

My street address has a letter on the end to make it unique:

"123D Memorial

Street". This works fine for mail delivery, it's what is engraved on the

mail boxes, and is more concise than "123 Memorial Street Apartment D", so

when I moved in "123D" is what I handed out as my new address.

Big mistake! While that address will work for a while (months), eventually

the businesses whose job it is to mail out magazines, notices, offers, etc,

will run clever software over their databases to "correct mangled addresses". When that happens, the "D" on the end gets deleted as an

"error", or (worse) changed into a "0". While mail addressed to "1230"

usually arrives, when presented with an address of "123" and a row of letter

boxes marked "123A", "123B", "123C", "123D", ... the mail carrier will

often just pick a random box to deliver the mail to.

This took a while to figure out. All I knew was that the amount of mail I

was getting seemed to be exponentially decaying. Calling up the magazines to

ask "are you sure you still have my address correct?" didn't work: in their

databases the "D" is invariably still there.

Eventually some of my own mail without the "D" ended up arriving in my box, so I was able to figure out what was happening. So now I have to call up everyone sending me mail and change my address to put the "Apartment D" on a separate line, where it is apparently stable. Even so I bet my neighbors will be getting all sorts of junk mail meant for me for months to come.

The risks?

Software that is overly aggressive in "fixing" addresses.

The address the subscription services people see in their computer is not the same as the one that is actually used (and they don't even realize it's not the same).

No error message being returned by the post office saying that the address without the letter can be delivered, but not reliably.

Purging all the "123 no D" addresses now existing in hundreds of databases out there will be just about impossible.

⚡ REVIEW: "Security Technologies for the World Wide Web", Rolf Oppliger

Rob Slade <rslade@sprint.ca>
Tue, 22 Feb 2000 10:49:32 -0800

BKSCTCWW.RVW 20000113

"Security Technologies for the World Wide Web", Rolf Oppliger,

2000,
1-58053-045-1
%A Rolf Oppliger rolf.oppliger@acm.org,oppliger@computer.org
%C 685 Canton St., Norwood, MA 02062
%D 2000
%G 1-58053-045-1
%I Artech House/Horizon
%O 800-225-9977 fax: 617-769-6334 artech@artech-house.com
%P 419 p.
%T "Security Technologies for the World Wide Web"

In the preface, the author states that the book is first intended for Webmasters, who need practical configuration information, then for users who have security concerns, and finally for Web and electronic commerce developers. He also says that the book can be used as an introduction, for self-study, as a course text, and as a reference. A pretty tall order, but, by and large, Oppliger does a reasonable job of fulfilling the entire mandate.

Chapter one, as an introduction, is possibly more than most people want to know. However, the extra information (such as the explanation of HTTP [HyperText Transfer Protocol] requests and responses) does help provide an understanding of the underlying actions and concepts which are needed for a thorough view of security operations and requirements. There is a detailed presentation of HTTP access control methods in chapter two. The introduction to firewalls, in chapter three, is complete and helpful, with a wealth of user level information that is all too often omitted. Chapter four is a solid introduction to the basics of cryptography. Channel security at the data link, transfer, and application layers is

the theme of chapter five, touching on tunneling, VPNs (Virtual Private Networks), IPsec, and various application protocols. Chapter six expands two of these with details on the Secure Sockets Layer (SSL) and Transport Layer Security (TLS).

Chapter seven gives an overview of electronic payment systems, with brief descriptions of the most common electronic cash, debit, and credit schemes. The management of certificates, in chapter eight, mostly covers ongoing work in key infrastructure, with a good discussion of the important and difficult question of certificate revocation. A fair and realistic review of active content is provided in chapter nine. For slightly less active content, chapter ten discusses and shows examples of more secure practices for CGI (Common Gateway Interface) and API (Application Programming Interface) work. Mobile code and agents are still really future technology, and so are the proposed security functions in Chapter eleven. The copyright discussion in chapter twelve is a little disappointing, since it seems primarily concerned with watermarking. Chapter thirteen looks at privacy, being dealt with by amateurs as usual, and, as usual, providing glimpses of fascinating work that is not widely known. There is a brief overview of censorship systems and problems in chapter fourteen. Chapter fifteen concludes with a somewhat pessimistic review of the situation.

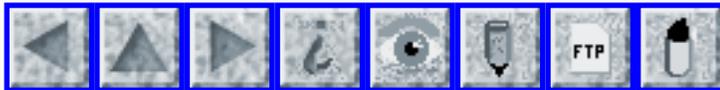
The bibliographies at the end of every chapter contain solid works, and can

be useful to those wanting further information. They do, however, have a very definite academic flavour, in that most of the entries are articles or conference presentations, with books and online references making up a smaller portion of the whole.

Oppliger's writing is rather dry and academic in tone, but the material presented is realistic, useful, and conceptually complete. Despite the disparate audience range, the author has managed to provide something of value for all. For the Web workers who are the primary audience, this book provides, if not a cookbook for security, a complete picture of the various aspects that must be addressed.

copyright Robert M. Slade, 2000 BKSCTCWW.RVW 20000113
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

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



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 83

Wednesday 8 March 2000

Contents

- [Gallup hacked](#)
[PGN](#)
- [Aum Shinri Kyo affiliate develops Japanese government software](#)
[PGN](#)
- [Computer releases prisoner](#)
[Bob Church](#)
- [Online broker blames outages on software maker](#)
[NewsScan](#)
- [Boeing loses space station parts](#)
[PGN](#)
- [Arizona primary is first binding election with Internet voting](#)
[Sidney Markowitz](#)
- [New Zealand's INCIS Crime Information System](#)
[Richard A. O'Keefe](#)
- [Risks of Web information on heart attacks](#)
[PGN](#)
- [Census fiasco](#)
[Bob Frankston](#)
- [UK ISPs leave themselves open to potential abuse](#)
[Pedt Scragg](#)

- [Judge sends message to network vandals: "go to jail"](#)
[NewsScan](#)
 - [The scary MSWord residue feature](#)
[Avi Rubin](#)
 - [Re: "Unstable" postal addresses](#)
[Peter Corlett](#)
 - [ADSL snooping](#)
[David](#)
 - [Risks of Leap Years and Dumb Digital Watches, quadrennial posting](#)
[Mark Brader](#)
 - [Leap-day 2000](#)
[Chris Kuan](#)
 - [Leap-day 2000: VCR](#)
[Bob Erkamp](#)
 - [Leap-day 2000: Checkbook magazine](#)
[Jeremy Epstein](#)
 - [Getting Jenni arrested](#)
[Keith Schon via sragdale](#)
 - [Privacy risks as mid-sized orgs decide that Web access is cool](#)
[Daniel P.B. Smith](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Gallup hacked**

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

Tue, 07 Mar 2000 21:31:34 -0800

The Gallup Organization's Internet site was hacked, shortly before today's primary elections. The hacked Web page appeared to be the work of John Vranesevich's AntiOnline, although JV denies it and Gallup also believes that his identity was spoofed. Gallup's 65-year historical polling data remained unchanged -- because their internal site won't be connected until 1

Sep 2000. But this certainly gives them an incentive to make sure their internal site is more secure.

[Source: Vandal alters Gallup Internet site just before primaries, cnn.com,

7 Mar 2000, courtesy of Dave Stringer-Calvert. See also

* On the Net: Gallup's Web site: <http://www.gallup.com>

* AntiOnline's Web site: <http://www.anti-online.com>

* Image of Gallup's hacked site:

<http://www.attrition.org/mirror/attrition/2000/03/05/www.gallup.com/>

I guess the archival history items might be known as "Gallup-agos".

Studying them tortoise a lot. PGN]

✶ Aum Shinri Kyo affiliate develops Japanese government software

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

Sun, 5 Mar 2000 14:15:01 -0500

An affiliate of Aleph, the cult formerly known as Aum Shinri Kyo (known for its nerve gas attacks in Tokyo subways), has apparently been a subcontractor

on Japanese Defense Agency contracts for the development of a secure communication network, and is suspected of planting a security trapdoor.

Police notified the Agency the day before operation was scheduled to begin.

The company also developed software for the Construction Ministry, the Posts

and Telecommunications Ministry, the Education Ministry, and NTT (among

others). This discovery follows on several recent attacks on Japanese

government Web sites, whose attackers were not identified.

[Source:

Doomsday Cult Linked to Government, 29 Feb 2000, courtesy of John Lowry.

<http://library.northernlight.com/EB20000229590000030.html?cb=0&dx=1006&sc=0#doc>

PGN-ed]

⚡ Computer releases prisoner

Bob Church <churchr@oak.cats.ohiou.edu>

Mon, 6 Mar 2000 13:06:21 -0500

The Southeastern Ohio Jail is a recently completed facility to serve four or five counties in Southeast Ohio. It was the subject of several news stories about delayed and poorly done construction. Executive Director Cochran publicly accused the contractors of "piddling around" instead of finishing work.

The following article appeared in the March 5, 2000 issue of the 'The Sunday Messenger' in Athens, Ohio.

Escaped Inmate Still at Large

An inmate who escaped from an unsecured door at the Southeastern Ohio Jail

Wednesday evening remained at large Saturday afternoon.

[descriptions of

Tharpe, accused of armed robbery of a carry-out and considered dangerous

...] Tharp was able to walk out of the jail when the emergency evacuation

system failed and unlocked all outside security doors to the jail, Cathy

Cochran, Executive Director explained. If the system would

have been

working correctly, a two-minute warning would have occurred before the

door unlocked and the officer on duty would either give the go-ahead or

discontinue the command. Instead the doors were unlocked automatically

and Tharp walked out. The alarm company that installed the system was on

the site Thursday and reviewed with officers a number of possibilities

that could have occurred. Regional Jail Captain John Morris said Friday

"to insure nothing like this incident could ever occur again, we have

taken all the fuses out of the outer security doors. Only officers with

keys will have the availability to unlock the door for exit purposes."

[The RISKS archives have a bunch of computer-related prison screwups.]

✶ Online broker blames outages on software maker

"NewsScan" <newsscan@newsscan.com>

Fri, 03 Mar 2000 08:56:53 -0700

National Discount Brokers, and online brokerage, says the outages it

experienced recently were the result of "hacker-like" attacks by an unnamed

Web software maker. The company had originally said its problems "had the

earmarks of a hacker attack." Apparently, the periodic disruptions were the

result of software incompatibility with products made by the outside company

that resulted in denial-of-service-type outages. NDB says it's considering

whether to pursue "appropriate judicial relief" through legal action against the company. The outages meant that NDB customers had to wait an average of 43.9 seconds to reach its site, twice as slow as the next slowest online trading site, and prevented 200,000 customers from placing stock orders online, although they could still relay orders over the phone. [<http://www.techweb.com/wire/story/reuters/REU20000303S0001> Reuters/TechWeb 3 Mar 2000; NewsScan Daily, 3 Mar 2000]

✶ Boeing loses space station parts

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

Mon, 6 Mar 2000 14:20:52 PST

Two nitrogen and oxygen tanks (worth \$750,000) still in their crates (5 feet on a side) for use by space-station astronauts were apparently accidentally sent off to the Huntsville dump after being moved outdoors temporarily to make room inside the Boeing plant. http://dailynews.yahoo.com/h/ap/20000303/sc/space_station_trash_1.html

✶ Arizona primary is first binding election with Internet voting

"Sidney Markowitz" <sidney@sidney.com>

Tue, 7 Mar 2000 13:09:31 -0600

The Associated Press has a fairly upbeat article about the Arizona

Democratic Primary as the first binding election in the US with votes cast over the Internet.

<http://www.mercurycenter.com/svtech/news/breaking/ap/docs/2882681.htm>

Other mainstream coverage is in Time

<http://www.time.com/time/digital/daily/more/0,2845,0,00.html>

The online voting is being conducted by Election.Com

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

But the darker side can be found at the Web site of the group that sued to

stop the online election, Voting Integrity Project,

<http://www.voting-integrity.org/>

where their case is made more strongly than in the brief summary of the AP article.

RISKS readers may be interested in the security of the voting process.

According to the elections.com website, each voter receives a PIN via postal

mail that gets them access to the voting web page. A voter also has to

answer "several questions" to confirm their identity. The instructions also

remind the potential voter that "[...] it is a Class 5 felony offense to

knowingly vote at an election when not entitled to do so." That is not the

same as verification of the identity of the person who knows the PIN and

knows the answer to the several personal questions, but then I've never had

to show a photo id when I have gone to a polling place to vote.

VIP's objections appear to have less to do with security and more with the

effects of unequal access by the poor and minorities who are less likely to

have a computer and an Internet connection. Easier voting for one group is seen to mean more voting power for that group.

Sidney Markowitz <sidney@sidney.com>

✶ New Zealand's INCIS Crime Information System

"Dr Richard A. O'Keefe" <ok@atlas.otago.ac.nz>

Thu, 09 Mar 2000 14:57:20 +1300

The New Zealand Police had 18 databases that were nearing the end of their useful life in 1990. They came up with the idea of combining them, plus a bunch of other stuff, to form the Integrated National Crime Information System. The business case was drawn up in 1993, and a contract signed with IBM in 1994. Last August, IBM pulled out, with only Increment 1 (of three Increments) completed. The project was three years late and running later all the time. The money was also blowing out: it was originally expected to cost NZD 80 million but was up to NZD 134 million when IBM pulled out. The government sued and IBM counter-sued, but that is now settled.

The Report of the Justice and Law Reform Committee on the CARD and INCIS

systems can be found at

<http://www.gplegislation.co.nz/incis/incis.html>

Since that report was issued last year, we have a new government, which has promised a fuller enquiry into the INCIS affair, but not the Royal Commission that many people were expecting.

About NZD 50 million of the cost was for hardware: 3000-odd PCs (although the amount spent on PCs seems rather higher than I would have expected), networks, buildings, and an S390 mainframe at about NZD 7.5 million, which the government now want to sell because it costs NZD 0.5 million/month to run. See

<http://www.govt.nz/news/detail.php3?id=400>

which has a link to a recent report on Police & Justice IT requirements.

Regular readers of comp.risks will find no real surprises in the report, including the fact that there are worries about data quality in the main Law Enforcement System data base (fields are not being used for their intended purposes, and the Courts don't bother filling some of the fields in anyway).

Quick summary:

- ambitious project (there wasn't anything like it available)
- customer demanded major architectural changes part way through
- requirements took a long time to discover
- customer kept asking for new features
- management problems (top level customer people who didn't get on, rapid project management turnover at IBM)

Mind you, it helped bring down the New Right government, so it's an ill wind as they say...

⚡ Risks of Web information on heart attacks

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

Wed, 08 Mar 2000 13:21:23 PST

The following letter appears on the Rochester General Hospital Web site

[http://www.viahealth.org/via_news/99_news/99_august_news/heartattack.html]

Important Notice Regarding the article
"How to Survive a Heart Attack When Alone."

Hundreds of people around the country have been receiving an e-mail chain

letter entitled "How to Survive a Heart Attack When Alone."
This article

recommends a procedure to survive a heart attack in which the victim is

advised to repeatedly cough at regular intervals until help arrives. The

source of information for this article was attributed to ViaHealth

Rochester General Hospital. This article is being propagated on the

Internet as individuals send it to friends and acquaintances - and then

those recipients of the memo send it to their friends and acquaintances,

and so on. We can find no record this was produced by Rochester General

Hospital. Furthermore, the medical information listed in the article can

not be verified by the medical literature. Please help us combat the

proliferation of this misinformation. We ask that you please send this

e-mail to anyone who sent you the article, and please ask them to do the same.

Sincerely, John Turner,
Director of Public Relations ViaHealth Rochester General Hospital

[This is of course not a unique case. I include it here simply

as one more reminder of the risks of unauthenticated e-mail. Incidentally, speaking of e-mail, the ever-vigilant French have

now rejected the use of the term "e-mail" (and many other terms)

as further incursions of American/English into francais. It is not

clear whether the fact that "email" is a perfectly good old French

word (relating to enameling) had anything to do with the matter.

(New RISKS readers in the past four years might want to look at

my lead note in [RISKS-17.95](#).) PGN]

✶ Census fiasco

"Bob Frankston" <rmf2gOther@bobf.Frankston.com>

Wed, 8 Mar 2000 11:36:35 -0500

Apparently all the informational mailings about the 2000 census [US] put an

extra digit before hour numbers so that 23 Main St can become 123 Main St.

Apparently the solution is to tell the postal workers to ignore the first digit.

Sounds reasonable except that this is the 2000 census and the real address

is in the barcode not the printed version. Seems similar to the assumption

that the Post Office made in changing some zip codes in 021 to 024 -- the

number is now a database key, not a physical delivery route.

So I looked a little further and saw

<http://www.census.gov/Press-Release/www/2000/cb00cn21.html> which said that the barcodes are, in fact, correct. So it is just a

minor
labeling error at the end point.

The real risk in news reports passing on factoids without understanding the underlying issues and thus giving a misleading report. Alas, this is the norm. The good news [NPI - No Pun Intended] is that they are not the sole gatekeepers of information even though the newspapers still don't provide links to their sources even if the source is a standard press release.

Of course, there's the whole issue of this being the last paper-based census but that is beyond the scope of riskoids.

Bob Frankston <http://www.Frankston.com>

⚡ UK ISPs leave themselves open to potential abuse

Pedt Scragg <pedt@signpost-design.co.uk>
Tue, 7 Mar 2000 17:41:46 +0000

A number of the new 'free' UK ISPs have left themselves open to potential abuse with certain e-mail/website addresses being available for the general public that should perhaps be not available.

I happen to be sysadmin@network-operations.freemove.co.uk and also network_operations@tesco.net amongst others - all via the signup page on their web sites and I get web sites to match the name.

Risks: I could put up a web site detailing non existent problems or post to

newsgroups using these addresses and they may well be believed as being from someone who works at the relevant NOC. Joe Public might well believe a site at <http://www.network-operations.freeseerve.co.uk> or at http://www.network_operations.tesco.net as being legitimate sites for the ISP if found on a Search Engine.

Pedt Scragg Signpost Web Design, Wreccsam, North Wales
<http://signpost-design.co.uk/>

⚡ Judge sends message to network vandals: "go to jail"

"NewsScan" <newsscan@newsscan.com>

Mon, 06 Mar 2000 07:59:23 -0700

Federal judge Irma Gonzalez has imposed an 18-month prison sentence on a 27-year-old man who as leader of a 12-member ring of network vandals broke into the computer systems of a number of major U.S. phone companies. In passing the sentence, the judge said: "This is a crime which is becoming more and more prevalent in our society. There has to be a message sent to this community that people like you, who commit this type of crime, will be punished." [AP/*San Jose Mercury News*, 5 Mar 2000; NewsScan Daily, 6 March 2000]

⚡ The scary MSWord residue feature

Avi Rubin <rubin@research.att.com>

Wed, 1 Mar 2000 21:16:53 GMT

I recently received a legal document as part of a personal negotiation that I am doing. The document was e-mailed to me in MSWord format. As I was showing it to my lawyer (who happens to be my wife), we decided to put our thoughts inline using the track changes feature of word. After selecting Tools, and Track Changes, we clicked on "Highlight changes in document" and voila, suddenly a whole bunch of red appeared on the screen. We looked at it closely and realized that everything in red represented changes in the document that my counterpart's lawyer had written. We got a good look at the previous version of the contract, as well as a bunch of comments and justifications that the lawyer wrote to his client. It was an eye opening experience.

It appears that instead of selecting "Accept all changes" before sending it to me, the other party to the contract simply turned off the highlighting to the track changes feature.

This is obviously a case of an unsophisticated person misusing a feature.

However, it is very dangerous. Lawyers send word documents around all the time, and many of them do not really understand all the features that they use, nor should they have to. I imagine that I was not the first person to see some behind the scenes conversation in an important word document, that I was never intended to see.

✉ Re: "Unstable" postal addresses (Re: Dellinger, [RISKS-20.82](#))

Peter Corlett <abuse@cabal.org.uk>

Sun, 05 Mar 2000 15:18:47 +0000

The UK Post Office exacerbates this somewhat by providing a database that will cleanse and correct addresses. This works by taking the house number and the post code, and generating an address in the preferred format for the Post Office. For example, the house number "234" and the post code "SW6 9XY" (that I've just plucked out of the air) might produce the address:

234 Random Street
Fulham
London SW6 9XY

This is quite a good scheme as it goes, since many companies seem to use it as an extra form of validation. If I phone a company who want my address, I'll be asked for my post code - which gives the street name and a range of house numbers - and will then be asked for my full address which they will cross-check on the screen. If it doesn't match, they know there's an error, and I'm asked to repeat it.

This is a great tool that stops misaddressing. Unless you're in a property that has been split into flats and has not been coded by the Post Office. For example, suppose 234 Random Street has been split into flats, and that I live in flat number 1. The proper address that I give out would thus be:

Flat 1
234 Random Street
Fulham
London SW6 9XY

Mail is successfully delivered to me at such an address. Unfortunately, some companies tend to lose the "Flat 1" because their database only has fields for "street address", "local area" and "post town", or try to use the 1 in the database, instead of 234. If you're lucky, 1 SW6 9XY is invalid, and it gets flagged. If not, your mail's going to go astray, being sent over a hundred doors down the road.

Other problems involve trying to bodge the "Flat 1" into the "street address" field of the database, since the database designer was a bit short-sighted. You will now see things put there as "Flat 1, 234 Random Street", or sometimes "1 234 Random Street". You'd better hope the postman's on the ball and there aren't a thousand houses on the street.

The Risk here is that some databases use aren't able to handle sub-addressing or free-form addresses, yet the designers still thought that their database would know somebody's address is what they claim it is. Time for a PO Box, I guess, let's see how they cope with that.

ADSL snooping

David <da0g+@andrew.cmu.edu>
Fri, 25 Feb 2000 11:01:41 -0500

On my ADSL system, with tcpdump, I've noticed traffic between two other machines. The traffic was not going through my system. But I was free to observe it, and snoop on the telnet sessions.

This was not normal. Bell Atlantic does not usually do this. (They have been informed, and will presumably take steps to correct this matter.)

However, it drives home the point that ADSL is **NOT** a substitute for decent security (ssh, kerberized services, etc).

⚡ Risks of Leap Years and Dumb Digital Watches, quadrennial posting

Mark Brader <msb@vex.net>

Tue, 29 Feb 2000 13:32:05 -0500 (EST)

All right now, how many people reading this...

-> saw a previous version of this message in [Risks 6.34](#), [13.21](#), or [17.81](#),

-> have watches that need to be set back a day because, unlike the smarter

kind of digital watch, they went directly from 28 Feb to 1 Mar,

-> and **hadn't realized it yet**?

Mark Brader, Toronto, msb@vex.net

⚡ Leap-day 2000

"Chris Kuan" <mrgazpacho@hotmail.com>

Wed, 01 Mar 2000 12:50:15 PST

My father's digital Casio wristwatch changed from Feb 29 to 30 Feb this year.

⚡ Leap-day 2000: VCR

Bob Erkamp <erkamp@arc.ab.ca>

Wed, 01 Mar 2000 09:17:39 -0700

I have a Sony SLV-940HF VCR with a nice feature that get's the date and time over cable from any channel that broadcasts it (I think it's PBS). I had programmed some shows to be recorded for Feb. 29/2000 and just happened to notice that the VCR wasn't recording when it should be. I checked my programming and the entries were there but the VCR wasn't taping? I then checked the date and time and it said it was Monday, February 28! The only way I could get me VCR to record anything yesterday was to switch to manual date and time. I am not sure which channel was broadcasting the incorrect time but I suspect others may have run into this?

Bob Erkamp, Alberta Research Council, 250 Karl Clark Road,
Edmonton, Alberta

T6N 1E4 CANADA 1-780-450-5181 <http://www.arc.ab.ca/individuals/erkamp/>

⚡ Leap-day 2000: Checkbook magazine

Jeremy Epstein <jepstein@monumental.com>

Wed, 1 Mar 2000 14:04:53 -0500 (EST)

I'm sure there are lots of these. Among them, Washington Checkbook magazine (a consumer magazine) seems to have sent out erroneous subscription renewals to some/all of their subscribers yesterday (February 29th). They sent out an apology e-mail, which is how I found out.

⚡ Getting Jenni arrested

<sragdale@my-deja.com>

Thu, 02 Mar 2000 18:21:05 GMT

[My friend Keith Schon <schon@supplybase.com> told me this story about

Valentine's day, and I offered to post it to comp.risks for him.]

I decided to send my girlfriend flowers for Valentine's Day, and I ordered them through the 1-800-Flowers website. Where the field says "enter card message" I typed "If I was there I would get myself a great big kiss from you." When the flowers arrived (3 days from the target date), the message on the card had been truncated by a few crucial words. The new mangled message left off my name and ominously said "If I was there I would get myself." One of her co-workers was sufficiently disturbed and called university security, who detained and questioned my girlfriend for most of the morning about stalkers, bomb-threats, etc. Basically I paid to have my girlfriend arrested.

I sent e-mail to their customer service department through the same website.

They advertised a response within 12 hours. 4 days later, I got a form

letter offering a partial discount, which showed no sign of their actually

having read my e-mail.

The RISK seems to be "be careful when you automate." If you're going to

rush the results out to customers before a human being checks them, at least

make good on your customer service. I'll never use these guys again via web

or phone, and I have a feeling they made a lot of their other V-Day

customers feel the same way.

✶ Privacy risks as mid-sized orgs decide that Web access is cool

"Daniel P. B. Smith" <dpbsmith@world.std.com>

Wed, 8 Mar 2000 13:43:38 -0500 (EST)

I belong to the singing organization SPEBSQSA (Society for the Preservation and Encouragement of Barber Shop Quartet Singing in America),

a nonprofit organization with about thirty thousand members and an

increasingly sophisticated Web operation.

Recently I received an unsolicited e-mail announcement of their "members

only" area. The e-mail, which of course wasn't secured in any way,

included a password for access to the account which happened to be a

single, correctly spelled English word six letters long. On accessing the

account I find that any member is, among other things, able to obtain the

chapter roster of any chapter, complete with names, addresses, home, work and fax phone numbers and e-mail address of every member in the chapter. (The chapters have to be accessed by their code number, but the code numbers are sequential and readily available in SPEBSQSA publications). At very roughly 1000 chapters and 30 members per chapter, it would be very feasible for a 'bot, or even a moderately patient human, to obtain the complete membership list for the entire organization.

There's no terribly sensitive information here, and of course there is the disclaimer: "The information contained on this site is confidential and may only be used for official SPEBSQSA business by authorized Society members. Unauthorized use of this site or the data it contains is strictly prohibited," which would presumably allow egregious abusers to be successfully sued. Still, this is AWFULLY sloppy.

The necessary expertise to make information available on a Web site is propagating an awful lot faster than the expertise needed to keep it secure. And the customary practice seems to be "_first,_ let the cat out of the bag; _then_ inform you that there's a cat and a bag."

Daniel P. B. Smith <dpbsmith@world.std.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 20: Issue 84

Saturday 18 March 2000

Contents

- [Report on hacker altering MIT grades: NOT!](#)
[Mark Lutton](#)
- [Radar glitch at Philadelphia's airport](#)
[PGN](#)
- [WAAS Software Problems](#)
[Peter B. Ladkin](#)
- [NASA report: Faster, cheaper is not better](#)
[PGN](#)
- [Sea Launch rocket drops satellite into Pacific Ocean](#)
[PGN](#)
- [Week-long outage after cable cut downs 11,000 phone lines](#)
[PGN](#)
- [Overdue Railtrack calls in the Army](#)
[Ursula Martin](#)
- [Hooked on I-sex](#)
[NewsScan](#)
- [Hackers sued by software-filtering company](#)
[NewsScan](#)
- [Y2K strikes again *R. Geoffrey Newbury\)](#)
- [Re: Arizona and Internet elections](#)

[Adam Shostack](#)

[Steve Wildstrom](#)

● [It was just a network board...](#)

[Wayne Mesard](#)

● [Risks of software configuration for filtering offensive language](#)

[George White](#)

● [Online gambling operator convicted](#)

[NewsScan](#)

● [The RISKS Of A Hyperactive Anti-Viral Immune System](#)

[Jon Seymour](#)

● [Risks of being a pushy high-tech headhunter](#)

[Michael D. Crawford](#)

● [Voicemail messages silently lost](#)

[Dick Karpinski](#)

● [Correction to privacy risks item](#)

[Daniel P. B. Smith](#)

● [Re: Web Information on heart attacks](#)

[Jeffrey Waters](#)

● [Info on RISKS \(comp.risks\)](#)

🔥 Report on hacker altering MIT grades: NOT!

Mark Lutton <mlutton@ma.ultranet.com>

Sun, 12 Mar 2000 21:03:46 -0500

On 9 Mar 2000, *The Boston Globe* reported that a hacker had broken into an MIT computer system and changed the grades of 22 students in a cell biology class. Some grades were raised and some were lowered but not in any sensible pattern. Teacher Harvey Lodish announced to his class (on Thursday March 2) that a cheating scandal had been uncovered. Suspicions did not point to any particular students in the class. No motive could be inferred

and it was believed that an unknown third party had done the hacking for no discernable reason.

On 10 Mar 2000, *The Boston Globe* reported that the mystery had been solved. The grades were recorded in a spreadsheet and a teaching assistant had unknowingly sorted the student name column without also sorting the grades columns. No intruder, no hack, no cheating scandal. Officials discovered the source of the mistake only after spending a full week ruling out the possibility of infiltration.

It seems to me that bound paper ledger books would be a much better tool for keeping grade records, at least for this teacher and his assistants.

Ref: www.boston.com, find Archives, search for "Lodish". Mark Lutton

✶ Radar glitch at Philadelphia's airport

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

Sat, 18 Mar 2000 17:15:12 PST

THREE times, on the evening of 10 Mar 2000, an almost-40-year-old air-traffic control radar system tracking arriving and departing planes malfunctioned, causing the identification tags of planes on radar screens to be blanked out. This affected about 30 planes on 8 screens, each outage lasting about three minutes -- although on recovery, the tags had to be manually reset by pilots, on request from the tower. Backup was available.

This followed on previous outages on 5 May and 17 May 1999.
[Source: noted
in the **Inquirer** by Andres Zellweger, and in **Infoworld** by
John McLean at
ubs.com. An unconfirmed report indicated that the malfunction
was due to
three ``processor cards''. PGN]

[An interesting question is whether the proposed new scheme of
a highly
distributed system that puts greater reliance on the computer
systems in
each cockpit will add to the risks or decrease them.
Distributed systems
tend to create risks not generally found in centralized
systems. PGN]

[Error in May dates fixed in archive copy. PGN]

✶ WAAS Software Problems

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>
Wed, 01 Mar 2000 17:15:05 +0100

AvWeek reported "software problems" with the Wide Area
Augmentation System
(WAAS) this week (28 Feb 2000, p49, story by Bruce Nordwall).
WAAS is a
ground-based system which will augment GPS positioning over the
continental
US to allow position accuracy to less than 3 meters (from 100
meters). This
will enable the FAA to develop near-precision instrument
approaches to
landing at airports that are not equipped with navigation aids,
for
properly-equipped aircraft.

WAAS accuracy was better than expected during tests (requirement

was 7.6m accuracy, but the system achieved better than 3m accuracy). However, integrity is the issue. The probability that a pilot would *not* get a positive warning when WAAS guidance is erroneous for longer than 6.2 seconds must be less than 1 in 10^{17} (units - I presume approaches). This evaluates to one in 47.5 years, apparently. *AvWeek* points out what most safety-critical-system professionals know and others can figure out in a second or two, that confidence to this level can only be achieved by analysis and not by testing.

The software problems were not detailed. However, two other problems uncovered during a 60-day stability test (that was terminated early) will be fixed through software. One is related to the switchover between the two ground-uplink stations. The other is multipath signal degradation at 5 of the 25 wide-area reference stations, that will be corrected through filtering software algorithms.

Peter Ladkin University of Bielefeld, Germany <http://www.rvs.uni-bielefeld.de>

✶ NASA report: Faster, cheaper is not better

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

Sat, 18 Mar 2000 17:01:57 PST

After the recent Mars probes were lost, shuttles delayed, the Hubble Telescope temporarily shut down, and other problems, NASA review

boards have concluded that the recent attempts motivated by ``Faster, Cheaper'' have been overzealous, with too little money and not enough oversight. [Source: AP item, 14 Mar 2000, PGN-ed]

✦ Sea Launch rocket drops satellite into Pacific Ocean

"Peter G. Neumann" <neumann@csl.sri.com>
Sat, 18 Mar 2000 17:14:41 PST

Launched from a converted ocean-going oil rig, a Russian-Ukrainian rocket carrying a British ICO Global Communications satellite (\$100M) fell into the Pacific after liftoff. This was a Boeing-led effort, after two previous successes -- a dummy test launch, and a DirecTV satellite. [Source: *San Francisco Chronicle*, 13 Mar 2000, A11, PGN-ed. No cause given. I hope some RISKS reader can provide details. PGN]

✦ Week-long outage after cable cut downs 11,000 phone lines

"Peter G. Neumann" <neumann@csl.sri.com>
Sat, 18 Mar 2000 17:09:10 PST

11,000 phone lines in northeastern San Jose were down for about a week on 10 Mar 2000, when a construction crew accidentally took out four buried cables. ``The repair work is mind-numbingly tedious, with each wire having to be spliced by hand and then tested.''' [Source: *San Francisco

Chronicle*,
14 Mar 2000, A13,18, PGN-ed]

⚡ Overdue Railtrack calls in the Army

Ursula Martin <ursula@csl.sri.com>
Sun, 12 Mar 2000 20:30:05 -0800 (PST)

[In [RISKS-20.67](#), we noted the Y2K glitch in Railtrack's on-line timetables. Much deeper problems have now arisen. PGN]

Privatised Railtrack is running about a year behind schedule and 3 billion pounds over budget in attempting to rebuild the London-Glasgow line. They have now turned to the Royal Logistics Corps and engineers ('`sappers'') from the Royal Engineers to teach Army discipline and consult on the repairs. Railtrack employees are being sent to Army training camps. Retired military folks are also being used as consultants. [Sources: The Telegraph, 13 Mar 2000 and 16 Dec 1999; PGN-ed]

Two quotes are noteworthy:

* Robin Gisby, of Railtrack, said: "We have expertise on rebuilding railways, but have never had anything as complicated as this line. We are using the Army because they have a lot of experience in moving men and materials to tight deadlines."

* Don Foster, Liberal Democrat transport spokesman, said: "After the trouble the Army has had with its rifles, let's hope they have more

success helping
to get the West Coast main line into action."

An earlier article explains that the cost overrun from 2.2 billion to 5.8 billion (that's UK pounds and UK billions) were due to the decision to abandon computerised "moving block" signalling, which removes the need for traditional lineside signals.

<http://www.telegraph.co.uk/et?ac=000125824864271&pg=/et/00/3/13/nrail13.html>

<http://www.telegraph.co.uk/et?ac=000125824864271&pg=/et/99/12/16/ntral16.html>

[URLs simplified in archive copy, TNX to Lloyd Wood. PGN]

Hooked on I-sex

"NewsScan" <newsscan@newsscan.com>
Wed, 01 Mar 2000 06:40:50 -0700

Psychologists from Stanford and Duquesne universities have published an article in the journal **Sexual Addiction and Compulsivity** claiming that at least 100,000 users are cybersex compulsives who spend more than 11 hours a week visiting X-rated Web sites and chat rooms. The study concludes: "This is a hidden public-health hazard exploding, in part, because very few are recognizing it as such or taking it seriously." The researchers believe that cybersex compulsives have difficulty maintaining normal relationships with others. [AP/**The New York Times**, 1 Mar 2000

<http://www.nytimes.com/aponline/a/AP-Online-Sex.html>; NewsScan

Daily, 1

March 2000

⚡ Hackers sued by software-filtering company

"NewsScan" <newsscan@newsscan.com>

Thu, 16 Mar 2000 09:21:14 -0700

Programmers Eddy L.O.Jansson and Matthew Skala are being sued by Massachusetts -based Microsystems Software, which produces and sells "Cyber Patrol" filtering software to protect children from pornographic content on the Internet. The lawsuit alleges the two men illegally "reverse-engineered" its software to create a "cphack" software utility to destroy the effectiveness of Cyber Patrol. Skala says he opposes Internet filtering software on philosophical grounds. [AP/San Jose Mercury News 16 Mar 2000)

<http://www.sjmercury.com/svtech/news/breaking/merc/docs/025265.htm>;

NewsScan Daily, 16 Mar 2000]

⚡ Y2K strikes again

"R. Geoffrey Newbury" <newbury@io.org>

Wed, 15 Mar 00 11:29:18 -0500

Robert Challender in Nevada registered his car late. He received a bill for \$378,426.25 from the Nevada Department of Motor Vehicles. After the mix-up was resolved, he wound up paying \$60. [Source: United States Agency puts

brake on bill, *National Post*, 13 Mar 2000, page A14. Of course, he was billed for accrued interest since 1900. I suppose the car should then have been re-registered as a horseless carriage, as per [RISKS-20.63-65](#). PGN-ed]

[I received an apology from my sewer pipe root removal service, which installed a new computer system last April, presumably for Y2K compliance. They *just* discovered they had missed my annual service last September. More than 6 months late. I hope they get to the root of the problem. PGN]

✉ Re: Arizona and Internet elections (Markowitz, [RISKS-20.83](#))

Adam Shostack <adam@zeroknowledge.com>
Thu, 9 Mar 2000 10:44:15 -0500

Regarding the Arizona elections, the election.com web page on confidentiality makes no promise that there will be no correlation of voters and cotes cast. Further, I'm unable to find a privacy statement of any sort on the web site. In light of recent revelations about 'democracy portals' gathering information, there seems to be a worrismatic chance that people's actual votes may be tallied, sorted, and stored in personally identifying formats. (Ross Kerber, *The Boston Globe Online*, 7 Mar 2000)

<http://www.election.com/political/arizona/security.htm>
<http://www.digitalmass.com/news/daily/03/07/database.html>

[Also, check out Lauren Weinstein's item on Internet voting, at <http://www.pfir.org>. PGN]

⚡ Re: Arizona and Internet elections (Markowitz, [RISKS-20.83](#))

"Steve Wildstrom" <steve_wildstrom@businessweek.com>

Thu, 09 Mar 2000 11:12:15 -0500

Voting is an unusual case where there is a simultaneous need for both authentication and privacy, and it's hard to see how both can be met. It's easy enough in the real world of physical ballots. In Maryland, where I vote, you sign in and are handed a set of ballots. Signatures are at least perfunctorily checked against the registration record, but I have never been asked for additional ID.

You vote the ballots in a punch machine. Before depositing the marked ballots into the ballot box, you tear off the numbered stubs which associate the ballots with your identity. This works nicely because the entire process is visible to, and understandable by, the voter. Once you are authenticated on line, how do you cast a secret ballot?

Steve Wildstrom, Technology & You Editor, Business Week, 1200 G St. NW Suite 1100, Washington DC 20005 1-202-383-2203
steve_wildstrom@businessweek.com

⚡ It was just a network board... (Re: [RISKS-20.80](#))

Wayne Mesard <Wayne.Mesard@east.sun.com>

Tue, 29 Feb 2000 14:27:37 -0500 (EST)

> a handful of network cards, costing about \$50 a piece, were
not able to
> handle [the Y2K witching dates], and were generating erratic
packets.
> Replacing the boards has fixed the problem, according to *Der
> Tagesspiegel*.

This story (or rather <http://babel.altavista.com/>'s translation
of same)

set off all my Urban Legend alarms. [Beat ya to the pun, PGN.]

Most of us have encountered bugs that looked and smelled like
one thing (due
to coincident or misinterpreted symptoms), but eventually turn
out to be
something else. Add to that the predisposition to blame
anything and
everything on Y2K, and you've got a recipe for miss-diagnosis.

I'm perfectly willing to believe that this is a Y2K bug. And
even that the
bug is with the network card as described in the article. But
first we need
more information:

- What was done to fix the problem on Jan 1? How did that fix
become

 - undone between then and now?

- Who is the manufacturer of this network card? Do they know
about

 - the problem? Do they agree that it is a Y2K bug? Why have
we only

 - heard of this single manifestation of the bug?

- Why is a network card aware of the date, anyway? (At \$50, I
doubt

 - there's any on-board encryption key management, for
example.) And

 - how could this information cause it to "generate erratic
packets"?

Without answers to these questions, I remain skeptical.

Wayne() ;

⚡ Risks of software configuration for filtering offensive language

George White <aa056@chebucto.ns.ca>
Sun, 12 Mar 2000 20:40:25 -0400 (AST)

The Royal Court, a UK theatre group known for vigorous opposition to censorship and for plays whose dialogue is intended to shock and offend, recently obtained a new computer system. This system was configured to prohibit entry of expressions that might violate standards appropriate to office e-mail systems in the US, much less dialogue of the sort for which the group is known. [Guardian Weekly, March 2--8, 2000].

George White <aa056@chebucto.ns.ca> Halifax, Nova Scotia

⚡ Online gambling operator convicted

"NewsScan" <newsscan@newsscan.com>
Tue, 29 Feb 2000 08:37:28 -0700

The first defendant to stand trial in New York for online gambling via offshore locations has been convicted. Jay Cohen, a U.S. citizen, ran an Antigua-based sports betting parlor called the World Sports Exchange. He was found guilty under a federal law against using telephone lines

to place
illegal wagers. Cohen faces up to five years in prison on a
conspiracy
charge and two years for each of seven sports betting counts.
[Bloomberg/*Los Angeles Times*, 29 Feb 2000;
<http://www.latimes.com/business/20000229/t000019506.html>;
NewsScan Daily, 29
February 2000]

✦ The RISKS Of A Hyperactive Anti-Viral Immune System

jon seymour <jon@zeta.org.au>
Sun, 19 Mar 2000 11:12:14 +1100

A friend was attacked by a worm the other day. This worm is a
Visual Basic
script that attempts to copy itself to every mapped drive it can
find, and
then some random ones besides.

Having found the worm, he created a copy of it, gave it a safe
file name and
then sent it to me as an attachment to an e-mail. His intent was
simply to
share a curio with me. He certainly didn't want to infect me
and thought he
had taken sufficient pre-cautions to prevent that occurrence.
And, in fact,
I was never infected. But the lack of a successful infection
does not mean I
didn't catch a nasty fever.

I use Windows NT, Netscape and don't have Visual Basic scripting
enabled. I
also have a popular virus checker installed with reasonably
recent list
files. You'd think I could read his mail safely without any
problems. You'd
be wrong.

What happened was this. As soon as I attempted to open my mail, I caught the title of the e-mail "I've been attacked by a worm". Then my mail client froze and several seconds later, the virus checker popped up and told me that my inbox had been infected by the worm and that it couldn't repair the file. So, I think, let's repair it manually. I shutdown Netscape and attempt to make a copy of my Inbox. Can't do it - access denied. Try to tail my inbox. Can't do it - access denied. Try to type my inbox. Can't do it - access denied. Not entirely sure what has happened at this stage, I start my scanner and ask it to do a full scan. 1 hour later it finishes. The only copy of the worm is in my inbox - it hasn't actually executed. But I still can't get at my inbox. So I figure I have to disable the virus checker. That doesn't work. So I reboot. Attempt to tail the file. The virus checker pops up again. Eventually, I manage to disable the virus checker, get access to the mail box, delete the offending mail item. Netscape would still not allow me to open my inbox. Then I realise it doesn't like some of the blank lines I left at the end when I did the manual edit, so I delete them too. Finally, 2 hours after the mail arrived, I could resume normal use of my system.

The RISKS? A worm can give you a nasty fever, even if it doesn't find a suitable execution environment. All it has to do is lure a hyperactive anti-viral immune system into acting.

jon.

PS: out of courtesy to fellow RISKS readers, I haven't added the worm as an informative attachment :-)

⚡ Risks of being a pushy high-tech headhunter

"Michael D. Crawford" <crawford@goingware.com>

Sat, 18 Mar 2000 07:14:41 -0800

While this isn't related to actual software failures I think it's probably relevant to the interests of most of the people who read this list, and the risk to the headhunters will become clear.

I used to get jobs and contract through recruiters and job shops regularly but lately I've been finding them especially pushy, crass and just plain ignorant. There are some who are quite good but these days they are definitely in the minority.

I also have found a lot of high-tech workers are taken advantage of by the contract firms, such as the fellow who posted to alt.computer.consultants about how he billed his agency at \$35/hour, and the agency billed his time to the client at \$90/hour, or my friend who was completely unqualified for a contract QA job, so the agency totally fabricated a new resume for him and sent him to the interview without mentioning the fraud, only to have it discovered by the client who asked for details on his exciting, relevant and completely fictitious job experience.

What really drove me over the top is that I got a "follow-me"

number for
my business but chose to let it go to voice mail while I've been
away
for the week visiting my desperately ill father. A recruiter
from
Oxford International called wanting me to do some smalltalk
work, which
I'd like to do but I'm not available, so I called back and left a
message saying I had a friend who might be interested in the
job, and
I'd check with her to find out.

Well this recruiter just blasted my business line off the hook,
scaring
my poor mom who was confused by the cryptic messages from the
follow-me
service. The recruiter, figuring that she wasn't going to get
through
on the business line, made the effort to track down my home
phone number
and then hounded my fiance to locate me, and leaving many
messages
demanding my friend's phone number.

My friend didn't want the job, and sure was adamant about not
giving out
her number after I described the recruiter's efforts.

I called the recruiter back, left a message saying she wasn't
going to
get my friend's phone number and recommended she go to my web
site and
read this page, which I've had up for quite a while, ever since
I came
to the firm conclusion that agencies weren't interested in
finding me
the kind of work I'm looking for:

<http://www.goingware.com/notes/recruiters.html>

Shortly after, a new consultant posted to alt.computer.
consultants about
how he just got into the business and wanted to know about

services that
find clients for a fee, saying he was just a programmer, didn't
know
about marketing, and was reluctant to make cold calls.

So I posted everything I knew about finding clients without going
through the agencies, and in fact have been doing totally
independent
consulting since April '98 without a single cold call.

I saved the post and then went to a lot of extra effort to write
it up
real nice in HTML and discuss what I thought of the state of the
recruiting business these days and posted it here:

<http://www.goingware.com/tips/marketing.html>

The main point of the page isn't just how to find clients - it's
how to
find clients without going through those obnoxious agencies.
It's about
taking back the power we were born with and using it to run our
lives
ourselves without allowing ourselves to be taken advantage of by
those
who would feed off of us.

I'm going to write a corresponding page soon to help employers
and
clients find employees and consultants without using agencies.

The short version: it's not rocket science. Get a web page. Put
keywords in it. Submit it to search engines and web indices -
clients
will find you when they do web searches. Use search engines and
web
indices to locate clients. It takes some effort but not really
that
much and actually it's kind of fun.

This is a particular case of what's discussed at the Cluetrain
Manifesto, which I highly recommend reading:

<http://www.cluetrain.com>

which (very briefly stated) points out that businesses that try to control the flow of information and do not serve their customers well will experience a backlash that is greatly aided and amplified by the free flow of information on the Internet, and the ready ability for customers (software consultants) to communicate directly with each other about things that such businesses (headhunters) would rather not have discussed publicly.

Mike Crawford crawford@goingware.com <http://www.goingware.com>

⚡ Voicemail messages silently lost

Dick Karpinski <dick@cfcl.com>
Mon, 13 Mar 2000 22:02:46 -0800 (PST)

Apparently some bugs survive change of ownership. Now that Octel is part of Lucent, I thought I'd see if they fixed the problem I was reporting perhaps five years ago. Looks like not:

I wrote this:

Years ago Octel voicemail replies had to be terminated with ## in order to be delivered. My efforts to get that changed were resisted at the time. Can you tell me if it is still so, please?

Lucent responded:

Hello Richard, I am personally unfamiliar with your prior request however, we have not changed the commands. Perhaps this was not explained adequately in the past. The first # ends the recording and allows for the entry of sending options, like private and priority, to be added to the message, and also, allows for deleting and re-recording the reply should the person wish to change what is in the content of the message. Then, the second # is the command to send the message. I believe it would be unlikely to change that in the future as the control functions after recording a reply are important and even mandatory.

If you wish to offer further suggestions, I would offer that sending them in to our Marketing and Engineering groups would be a good route as they are constantly looking at ways to improve our products.

> Thank you for your question and interest in Lucent Technologies, voice messaging products.
> Roger J. Miller
> Manager, Messaging Technical Services Organization
> Lucent Technologies

So I wrote:

I shall do as you say, but I personally request that you consider the plight of the average guy using the system. If he's not really well trained in replying to voice mail, he may treat it as if it were voice mail. That is, when he's done talking to the machine, he hangs up.

The problem is not even that such messages are unceremoniously dumped. The

problem is that the message is lost AND NO ERROR IS INDICATED.
A guy can go
for months telling people he DID return their voice mail while
they tell him
they never got it.

It wouldn't take a big change to fix the problem, but all the
experts chalk
up the failures to inadequate training. I chalk it up to a
BROKEN user
interface that allows slightly forgetful users to go on making
mistakes for
a long time.

This makes the whole organization seem stupid or irresponsible.
It may die
the death of a thousand cuts. This is not a trivial matter. They
are your
customers and they deserve better.

Yours for a better world,

Dick Karpinski The world's largest leprechaun. |=|:-}=

PS. Could you let me know how to reach your Marketing and
Engineering
groups to suggest the change?

✶ Correction to privacy risks item ([RISKS-20.83](#))

"Daniel P. B. Smith" <dpbsmith@world.std.com>
Tue, 14 Mar 2000 06:34:30 -0500 (EST)

I recently cited SPEBSQSA, a non-profit organization to which I
belong, as
an exemplar of a tendency of more and more organizations to
casually roll
out Web sites with privacy risk exposure on an "automatic" or
"opt-out"

basis.

My item on SPEBSQSA contained a factual error. I criticized their members-only web site for making chapter rosters available, with name/address/phone information. This information is in fact only made available to registered Chapter officers. This reduces the privacy risks and means that the Web site's privacy policy is similar that of SPEBSQSA.

This restriction is not obvious to a casual observer, but I should have checked this specifically before submitting this item to RISKS.

Apologies to those concerned.

Daniel P. B. Smith <dpbsmith@world.std.com>

[This correction is included in the interest of barber-shop harmony. PGN]

✶ Re: Web Information on heart attacks ([RISKS-20.83](#))

"Jeffrey Waters" <jeffreyw@htimes.com>

Thu, 09 Mar 2000 08:22:47 -0600

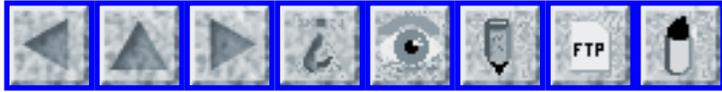
I would encourage Mr. Turner to review the current manuals used by the American Heart Association for training health-care providers in BLS (Basic Life Support) CPR. This document does mention the coughing routine. As I recall, it does not endorse this method but does outline what purpose the coughing serves.

I would hope the ER department at RGH will have a few words with

Mr Turner.

And if he has a heart attack, by all means, don't let him cough!

J Waters



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 85

Friday 24 March 2000

Contents

- [Northwest grounded for 3.5 hours after cable cut](#)
[Tim Dixon](#)
- [Patriot fails again](#)
[Lord Wodehouse](#)
- [Iridium insidious](#)
[PGN](#)
- [Leap-day banking ALERT!](#)
[Harlan Rosenthal](#)
- [Weather.com leaves visitors in the cold](#)
[Jay D. Dyson](#)
- [Cybercrime losses double to \\$10 billion](#)
[NewsScan](#)
- [Massive credit-card theft exposed](#)
[NewsScan](#)
- [Hacking credit cards is preposterously easy](#)
[Martin Minow](#)
- [Laptop Security](#)
[Steve Loughran](#)
- [Risks of Microsoft Passport](#)
[Avi Rubin](#)

- [Actor sues eBay for causing identity theft](#)
[Jim Griffith](#)
 - [Re: MIT grade spreadsheet problem](#)
[Wm. Randolph Franklin](#)
 - [There *still* ain't no such thing as a free lunch](#)
[Malcolm Pack](#)
 - [Re: Hackers sued by software-filtering company](#)
[Bear Giles](#)
 - [Re: Internet voting](#)
[Adam Shostack](#)
 - [Report raises online privacy concerns](#)
[NewsScan](#)
 - [TWA includes e-mail others' addresses in bulk mailing](#)
[RA Downes](#)
 - [Re: Overdue Railtrack calls in the Army](#)
[Mark Nelson](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Northwest grounded for 3.5 hours after cable cut

Tim Dixon <tdixon.no@spam.fwi.com>

Wed, 22 Mar 2000 19:14:26 GMT

When will people learn? Computerworld reports that Northwest Airlines had to cancel about 130 flights during a 3.5-hour outage at their Twin Cities hub. It seems a contractor accidentally bored into the cable cluster containing both main and redundant fibre lines.

[<http://www.computerworld.com/home/print.nsf/CWFlash/000322CBDE>]

When will people learn they need to know where their redundancy lies?

Cables run through the same conduit are only partially redundant, as events

like this will happily take out all the cables in a conduit, making the conduit itself a single point of failure.

[It sure is a common thread in RISKS! Thanks to the others of you who noted this case also. PGN]

✶ Patriot fails again

Lord Wodehouse <w0400@ggr.co.uk>
Fri, 24 Mar 2000 16:38:04 +0000

>From the BBC:
http://news.bbc.co.uk/hi/english/world/americas/newsid_689000/689329.stm

Yet again the Patriot missile has hit the news. Again units on high alert status for long periods have developed problems.

Tests have shown that missiles kept constantly on high alert have developed problems in receiving a radio frequency downlink, which guides the missiles in flight.

General Kern said the Patriot's manufacturer, Raytheon Co., had guaranteed that the missiles would work properly if on high alert for a maximum of six months.

The full article provides ore details. However the risks are 1) the missile fails when required to work (seen before in the Gulf War) and 2) people believe that the missile works, when it may not. The former means it is a less reliable form of defence and the latter means people might assume they are safe.

[Of course checking the Raytheon web site shows nothing about this on the top page. A search of their site does not seem to feature the story either. Another risk here: absence of information. John]

Global Research Information Systems, Glaxo Wellcome, Gunnels Wood Road, Stevenage SG1 2NY UK +44 1438 76 3222 <http://ds.dial.pipex.com/lordjohn/>

✶ Iridium insidium

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

Thu, 23 Mar 2000 7:55:01 PST

Jo Le Guen, the Frenchman who is rowing solo across the Pacific, six weeks into a four-month trip from NZ to Cape Horn in Chile, in hopes of raising awareness of the plight of our oceans.

[<http://www.wired.com/news/print/0,1294,35077,00.html>]

Rune Gjeldnes and Torry Larsen, two Norwegians, are attempting to be the first known to ski from Russia to Canada over the North Pole.

[http://dailynews.yahoo.com/h/nm/20000320/tc/iridium_norway_1.html]

What do they have in common? Both efforts may lose their communications lifelines when the plug is pulled on the Iridium satellite network at midnight on 24 Mar 2000, after Iridium LLC failed to be rescued from bankruptcy. However, Motorola will attempt to keep the network running in remote areas "for a limited period of time." Le Guen gets his

weather

forecasts from France, and talks with his doctor. (He has some alternative modes of communication, but with practical restrictions.)

[Thanks to Mark Brader and George Mannes for the source material.]

⚡ Leap-day banking ALERT!

Harlan Rosenthal <H.Rosenthal@Dialogic.com>

Wed, 22 Mar 2000 09:37:17 -0500

This came from one of my staff. - harlan

> Check the bank statements carefully this month!!!

> My bank missed a posting made 29 Feb 2000.

>

> I was about to panic when I checked with the company to be paid - they did

> have the payment, received 29 Feb. My bank account statement went from 28

> Feb to 1 Mar, the payment wasn't shown, and it looks like the amount was

> not accounted for.

⚡ Weather.com leaves visitors in the cold

"Jay D. Dyson" <jdyson@techreports.jpl.nasa.gov>

Mon, 20 Mar 2000 08:09:52 -0800 (PST)

The risk here? Total reliance on a website. Fortunately, my reality check

(an open window) gave me the 0day info on the genuine weather conditions.

This morning, I was told by my sweetie to go look at <http://www.weather.com/> to see what the daily forecast is. You can only imagine my surprise when I saw this week's forecast for ZIP code 91109!

<http://www.weather.com/weather/us/zips/91109.html>

TODAY	Windy	hi 18F
	lo 7F	
TUE	Partly cloudy	hi 19F
	lo 9F	
WED	Partly Cloudy	hi 21F
	lo 9F	
THU	Partly Cloudy	hi 22F
	lo 9F	
FRI	Mostly Cloudy	hi 22F
	lo 9F	
SAT	Showers	hi 19F *
	lo 8F	
SUN	Partly Cloudy	hi 22F
	lo 46F	

* I'd like to know how we're going to have "showers" when it's

19 degrees F, too.

Now either I'm re-acclimated to Iowa-like weather very darn quick, or the database is mixed up between Celsius and Fahrenheit. This parka of mine is just too darn warm, I tell ya!

Thanks go to my sweetie for mentioning this to me this morning, otherwise I'd have froze to death! ;)

Cybercrime losses double to \$10 billion

"NewsScan" <newsscan@newsscan.com>

Wed, 22 Mar 2000 08:25:15 -0700

Financial losses attributed to malicious hacking, online corporate espionage and other computer crimes probably doubled last year, according to a survey by the Computer Security Institute. The survey covered 643 major corporations and public agencies that estimated their computer crime losses at \$266 million in 1999. Based on that number, CSI estimates that total losses attributable to computer crime are around \$10 billion annually, mostly from financial fraud and proprietary information theft. However, only one company in four surveyed reported the crimes in 1999, down 32% from 1998. Suspected reasons for the decline are fear of bad publicity and distrust of the FBI. Based on the survey responses, 59% of the companies said the computer attacks initiated from the Internet, while 38% said they initiated from internal company computers. [*Los Angeles Times*, 22 Mar 2000, <http://www.latimes.com/business/20000322/t000027053.html>, NewsScan Daily, 22 Mar 2000]

✶ Massive credit-card theft exposed

"NewsScan" <newsscan@newsscan.com>

Fri, 17 Mar 2000 09:43:17 -0700

In Jan 1999, a computer vandal stole information on 485,000 credit cards from an e-commerce site and then secretly stored them in a database on a

U.S. government agency's Web site. Although the theft was discovered in March 1999 when a government administrator noticed that "a lot of the memory (on the Web site) was chewed up for no reason, so he checked and found the file (containing the stolen data)," many of the credit cards remain in use today because credit-card companies and card-issuing credit unions decided that it would be too much trouble to shut down the accounts and issue new numbers, according to an unnamed source. There is no evidence that the any of the cards have been used to commit fraud, and Secret Service spokesman Jim Macken says investigations point to an Eastern European perpetrator. It's unclear why the data was deposited on a government Web site, although Macken suggests that it may be the online equivalent of thumbing one's nose at U.S. authorities. [MSNBC 17 Mar 2000 <http://www.msnbc.com/news/382561.asp> NewsScan Daily, 17 Mar 2000]

✶ Hacking credit cards is preposterously easy

"Minow, Martin" <martin.minow@thinklinkinc.com>
Fri, 24 Mar 2000 08:39:16 -0800

The Register <<http://www.theregister.co.uk/000324-000017.html>> reports that is is "preposterously easy" to hack many sites that collect credit card information.

One computer enthusiast well known to The Register, who goes by the alias

'Ksoze' (as in Kayser [Kaiser?] Soze), shows particular contempt for the security of the popular CGI log-in forms which enable consumers to enter their credit details when making a purchase on line. These Perl scripts are ripe for exploitation -- the real low-hanging fruit of the IP jungle.

... It's all too easy: "Just hit 'update account' and you get the form as filled in by customers," he says.

``**** are thieves, OK, but they're morons too. They supply a CGI to their customers named ccbill-local.cgi by default. Site administrators need that CGI to add users, update accounts, and so on; but **** supplies the CGI chmod-ed as world-readable, in a world-readable directory! Aren't they totally lame?''

Transcribed (with the CGI vendor name removed) by Martin Minow, minow@pobox.com

[Credit-card fraud worldwide is reportedly just under \$1 billion a year, at about .7 percent of gross, but that represents only about 2% of banking losses. Private communication. PGN]

Laptop Security

"Steve Loughran" <slo2@iseran.com>
Fri, 24 Mar 2000 14:03:25 -0000

The BBC on line news, 24/March/00 covers an embarrassing laptop theft

http://news.bbc.co.uk/hi/english/uk/newsid_688000/688814.stm

MI5 laptop snatched

Special Branch detectives are searching for a computer containing sensitive information on Northern Ireland after it was stolen from an MI5 agent. The 2,000-pound laptop was snatched as the agent stopped to help a passer-by at Paddington Underground station in central London. Its data was encrypted and security officials are thought to be confident it could not be accessed.

The article continues with some opinions on how there is no such thing as a ``completely safe encryption system'', and the implications of the loss.

One must hope that the ``hibernate'' partition and swap file of the notebook is also suitably encrypted, and that in the unlikely event that they are using Windows 2000's encrypting file system, that all the files have innocuous names.

As a recent Microsoft knowledge base article describes: <http://support.microsoft.com/support/kb/articles/Q248/7/23.ASP> , their encrypting file system only encrypts the contents of files, not the file names. Whereas an encrypted file ``secret plan to subvert the government.html'' would not be readable, the fact that you had a secret plan would be widely known...

-Steve

Avi Rubin <rubin@research.att.com>

Tue, 21 Mar 2000 14:33:05 GMT

Dave Kormann and I took a look at Microsoft's Passport protocol and examined the risks. Our full paper is available at

<http://cs.nyu.edu/rubin/passport.html>

Here is the abstract:

Passport is a protocol that enables users to sign onto many different merchants' web pages by authenticating themselves only once to a common server. This is important because users tend to pick poor (guessable) user names and passwords and to repeat them at different sites. Passport is notable as it is being very widely deployed by Microsoft. At the time of this writing, Passport boasts 40 million consumers and more than 400 authentications per second on average. We examine the Passport single signon protocol, and identify several risks and attacks. We discuss a flaw that we discovered in the interaction of Passport and Netscape browsers that leaves a user logged in while informing him that he has successfully logged out. Finally, we suggest several areas of improvement.

Avi

Actor sues eBay for causing identity theft

Jim Griffith <griffith@netcom.com>

Tue, 21 Mar 2000 14:17:58 -0800 (PST)

Jerry Orbach ("Law and Order", `_DIRTY DANCING_`, `_FX_`, and many others) is suing eBay for allegedly allowing a user to auction two of his old acting contracts. Reportedly, the scanned images of the contracts showed his Social Security number, which allegedly resulted in credit card fraud.

<http://www.cnn.com/2000/SHOWBIZ/News/03/21/showbuzz/#story2>

✉ Re: MIT grade spreadsheet problem (Lutton, [RISKS-20.84](#))

Wm. Randolph Franklin <wrf+risk@mab.ecse.rpi.edu>

Tue, 21 Mar 2000 17:38:49 -0500

That sort of problem is a constant worry to large-course coordinators, who have to assemble grades submitted by various graders into one database, while adding and deleting students from the classlist. As students are added, formulae must be copied, relatively, and summation ranges must be extended. One wrong mouse click can invisibly drag a cell somewhere else.

One obvious check, which was not made, is to sample a few students, and check for reasonableness. An after-the-fact check is to give the students complete info about the inputs and outputs for their individual grades. However, that's not so easy. At times, I've used nested shell scripts to e-mail each student. At other times, I've created a separate AFS directory

for each student, permitted to only that person.

One deep reason for the problem is as follows. It's hard to destroy or mutilate info on paper. It's easy to delete info from a computer file.

This sort of user interface and metaphor problem is one of the areas in which Computer Science has not advanced in decades.

Does anyone remember the Florida contractor who used Lotus to prepare a bid, which was too small since his summation range was too small? He won the bid, then sued Lotus, leading to a cover story in (I think) Business Week.

Wm. Randolph Franklin wrf+risk@mab.ecse.rpi.edu (PGP available)

<http://www.ecse.rpi.edu/Homepages/wrf/>

[WRF is undoubtedly referring to the SYMPHONY case:
Lawsuit vs Lotus' Symphony dropped (omitted General Costs proposal section)(ACM Softw.Eng.Notes 11, 5, RISKS section, pp.11-12, October 1986, and SEN 12 1, January 1987. PGN]

⚡ There *still* ain't no such thing as a free lunch

Malcolm Pack <mpack@email.com>

Sun, 19 Mar 2000 08:05:19 +0000

On 14 Mar 2000, Stephen King's latest Novella, published only as an Electronic Book, was made available "free of charge" by Barnes and Noble on the company's web site. Thanks to recent upheavals in the UK Telco/ISP marketplace, for once this truly was a "free" offer, since I would be able

to download the book without incurring metered telephone call charges.

The book was available in three formats:

- o RocketBook

Only for owners of a NuvoMedia's physical Rocket Book device. Those of us in possession of the eBook software were SOL.

- o GlassBook

A new (to me) format that required the download of a free-of-charge reader that includes Adobe PDF technology,

- o Adobe PDF

To be sent by e-mail.

Having discovered that the Rocket edition was not available to me, I requested an e-mail copy (for which I am still waiting) and decided to download the free GlassBook version with its free viewer.

I won't go into the length of time it took to connect to clearly- overloaded servers at bn.com and glassbook.com. Needless to say, I was not permitted to get the book until I had finished downloading the 7MB reader, which I eventually managed to do, and installing it.

The reader installed, and asked me to reboot my Windoze NT4 SP6a PC to enable it, which I did. The PC restarted, got to the "blue startup screen", restarted itself, got to the "blue startup screen", restarted itself, got to the "blue startup screen", restarted itself, got to the "blue startup screen", restarted itself...

Two hours, and much detective work later (thanks to my being able to dual-boot into SuSE Linux and see my NT partition outside its

crippled OS
host), the culprits turned out to be a SYS and a VXD (tpkd.*)
that the
software had installed. Both were "InterLok(R)" files created
by "PACE
Anti-piracy, Inc". My PC had been crippled by anti-piracy
measures applied
to a "free" software product I'd installed to read a "free"
book. It is
entirely feasible that others were locked out of their systems
for good by
this software.

Epilogue

Fortunately, some things in life *are* free (if one owns the
right
Advertisement-blocking software ^-^), so I was able to use
dialpad.com to
telephone the US-based support desk for Glassbook using my PC as
a
telephone. After a 30 minute hold, I was put through to a
technician, and
explained the problem. While sympathetic, the response boiled
down to "This
is Beta software. I'll log the report for action."

I've heard nothing since, and I still haven't got a copy of the
book.

Malcolm Pack <mpack@email.com>

✦ **Re: Hackers sued by software-filtering company ([RISKS-20.84](#))**

Bear Giles <bear@coyotesong.com>

Mon, 20 Mar 2000 09:25:32 -0700 (MST)

There is *far* more going on here than meets the eyes. Those
programmers

are involved in the Peacefire anti-censorship group (<http://www.peacefire.org>). The site has had detailed instructions for getting around censorware software for months, without any legal action from the companies.

But for some odd reason Symantec (I-Gear) threatened legal action only after Peacefire cracked their encrypted blacklist and determined that 76% of the sites in a quick sample (the first 50 .edu sites) were erroneously blocked.

Likewise Mattel (CyberPatrol) sued only after Peacefire cracked their encrypted blacklist and published the results.

To a critical mind, several questions scream out:

- why are the blacklists encrypted? Is this to block access by competitors, or is it really to prevent parents and libraries from performing their own quality checks? (If it's an anticompetitive measure, why are the companies treating it as a "hackers, kids and porn" case?)
- how would knowing that a site is on the blacklist permit a kid to access the blocked site? How many kids have the technical knowledge to edit the blacklist... and how hard would it be to check an MD5 checksum every so often? (Since the blocking software only works when the computer is on the 'net, it is trivial to automatically download the checksum every Nth request. If they don't match, download a new copy of the blacklist.)
- why would the legitimately blocked sites have a problem with this?
AFAIK most legitimate porn sites are more than willing to cooperate

with censorware companies because it reduces their legal exposure -

they can demonstrate a good-faith effort to prevent access by minors.

The only sites that have a beef with this issue are ones that are

blocked due to judgement calls, e.g., the pro-censorware Christian

group that was was shocked to discover itself on a blacklist because

of its firm, principled stand against homosexuals and heathens.

Further complicating the issue is the apparent attempts to invoke the DMCA

(essentially criminalizing political debate if one party uses even trivial

encryption of key evidence; it brings to mind the 80's fad of putting a

lawyer into every meeting so the company could claim lawyer-client

confidentiality) and the pending UCITA legislation (which would explicitly

criminalize badmouthing software). And we must never forget the absurdity

of a U.S. judge telling a Swedish ISP that it can't host material for two

Canadian residents - do all courts have worldwide jurisdiction in the

pre-natal millennium?

I strongly recommend anyone interested in this topic review the Censorware

Project's report on an analysis of the logs of all Utah schools and

libraries. (<http://censorware.org/reports/utah/>) This report has been widely

misquoted as proving that censorware works. The 0.0006% (or "1-in-6

million," as was allegedly misquoted at one point in the Bush-McCain

slugfest) error rate is a total fiction; any sane analysis shows that about

1-in-20 blocked sites are blocked in error in practice.

*** Late update: according to Slashdot

(<http://slashdot.org/article.pl?sid=00/03/20/0845236>) Mattel

(CyberPatrol)

has not only sent mass mailings to all mirrors of the the critical webpages,

they have allegedly added these mirror sites (and the author's homepages) to

their blacklist *under all categories.* Slashdot also reports that Declan

McCullagh, respected journalist for Wired who has never hosted the essay

in question has also received legal threats.

This means there is an excellent chance that this issue of comp. risks will

be unavailable to school children nationwide due to its shocking content of

nudity, explicit sexual depictions, violence, drug use, satanic acts,

gambling activities, etc.

The RISKS created by an "informed public debate" on the merits of censorware, where the library patrons are quietly "protected" from

legitimate criticisms of one side of the debate should be obvious to

everyone. This is *not* an example pulled out of thin air -- another recent

Slashdot discussion covered the Holland, Mich. debate on whether to mandate

this type of censorware in their libraries. One can only shudder in

anticipation of the glorious day when nobody is even aware of this problem

as DMCA and UCITA ensure that no software, anywhere, ever has any publishable defects of any kind.

On the bright side, this one petulant act may be enough to raise serious

constitutional issues of whether it will *ever* be legal for a government to

mandate the use of censorware on publicly access systems. If this nonsense is allowed to stand, we might as well appoint the CEO of Mattel Lord High Emperor because he(?) will have demonstrated the ability to stifle the free political debate that lies at the heart of our democracy.

(The preceding political screed was brought to you by the Drug-Running Child Pornography Terrorists of America.)

Bear Giles <bgiles@coyotesong.com>

P.S., some people are already calling for a Barbie-Q to protest this. I am seriously torn between the attraction of torching a little Mattel CEO-in-drag effigy on the steps of the state capitol (and passing out flyers explaining the situation to passing legislators) and the horrid fact that that means Mattel would get even one thin dime from me.

[Does Barbie have a Mattelephone? PGN]

🔥 Re: Internet voting ([RISKS-20.83-84](#))

Adam Shostack <adam@zeroknowledge.com>
Sun, 19 Mar 2000 12:53:10 -0500

Regarding the question Steve Wildstrom poses in [Risks 20.84](#), "Once you are authenticated on line, how do you cast a secret ballot?"

One answer lies in a set of technologies called minimal disclosure credentials. These were invented by David Chaum, and substantially enhanced by Stefan Brands. The core of it is, you authenticate to some

server, and are granted a single-use credential which can not be linked to your authentication. The inability to link back to the authentication is provided by a technique called blinding, where the client takes a set of actions to prevent the server from knowing what it is signing. This technique forms the basis for anonymous electronic cash, and can be used to create a 'coin' whose value is 'one vote.' The state can allow each voter to withdraw one coin, and ensure that each vote is 'paid for' with one valid coin, thus assuring one person, one ballot, per election. (This proposal has a number of flaws, but is useful as a straw man if you understand electronic cash.)

Schneier's Applied Cryptography, chapter 6, has a long list of electronic voting protocols and systems which are intended to address these types of questions.

Adam

[Wait until you see Bruce's next book, forthcoming, which takes a less sanguine view of good crypto protocols in the presence of flawed implementations or weak system embeddings.

Incidentally, Lauren Weinstein called to my attention an article on

Arizona's experience with Internet voting that is of interest here:

<http://www.washingtonpost.com/wp-dyn/politics/A37369-2000Mar18.html>

PGN]

✦ Report raises online privacy concerns

"NewsScan" <newsscan@newsscan.com>

Thu, 09 Mar 2000 09:57:08 -0700

A new Justice Department report, titled "The Electronic Frontier: The Challenge of Unlawful Conduct on the Internet," has put privacy activists on alert: "What the report amounts to is a law enforcement Internet wish list of ways in which they can strip away privacy and free-speech protections in order to get at what they claim is this criminal element online," says an ACLU spokeswoman. The most controversial part of the report is a passage that terms anonymous e-mail a "thorny issue": "Given the complexity of this issue, balancing the need for accountability with the need for anonymity may be one of the greatest policy challenges in the years ahead." A White House deputy press secretary attempted to reassure ACLU officials, saying the administration understands the importance of privacy, including the positive role anonymity can play in reporting crimes and war atrocities. [*The Washington Post*, 9 Mar 2000, <http://www.washingtonpost.com/wp-srv/business/feed/a39970-2000mar9.htm>;

NewsScan Daily, 9 Mar 2000]

✦ TWA includes e-mail others' addresses in bulk mailing

<main@radsoft.net>

Wed, 22 Mar 2000 05:37:51 +0000

[TWA accidentally disclosed e-mail addresses of 80% their customers, albeit in alphabetically ordered batches. Spammers's delight? Advertiser's boon? Violation of their privacy policy? PGN]

Again, mice prove to be erratic creatures:

<http://news.cnet.com/news/0-1007-200-1580221.html?tag=st.ne.ron.lthd.1007-200-1580221>

It would seem a standard "Are you really really sure?" would be in order here so that the mice don't take the day.

-R

Radsoft Laboratories <http://www.radsoft.net>

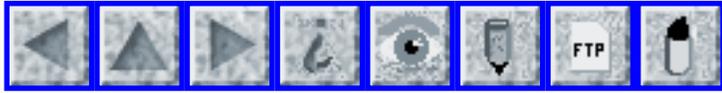
⚡ Re: Overdue Railtrack calls in the Army (Martin, [RISKS-20.84](#))

"Mark Nelson" <mnelson@fnx.com>

Wed, 22 Mar 2000 11:58:35 -0500

> An earlier article explains that the cost overrun from 2.2 billion to 5.8 billion (that's UK pounds and UK billions)

[We have been around this one before in RISKS. For quite a few years, UK billions and and US billions have been unofficially the same, irrespective of whether OFFICIALLY the UK billion might still be a million million. I had inteded to take out Ursula's unofficially gratuitous parenthetical. 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 20: Issue 86

Thursday 30 March 2000

Contents

- [More NASA woes in stress testing](#)
[PGN](#)
- [Re: Faster, cheaper *not* better](#)
[PGN](#)
- [More details on the Sea Launch failure](#)
[Steven Huang](#)
- [Stephen King eBook cracked \(Re: Pack, \[RISKS-20.85\]\(#\)\)](#)
[PGN](#)
- [California privacy legislation](#)
[Dan Gillmor](#)
- [Criminal records in North Carolina](#)
[Joe Thompson](#)
- [Judge issues injunction in software reverse-engineering case](#)
[NewsScan](#)
- [Re: Hackers sued by software-filtering company](#)
[PGN](#)
[Ross Oliver](#)
- [German ministry of family et al. and links to porn](#)
[Klaus Brunnstein](#)
- [Privacy problems with HTTP cache-control](#)

[Martin Pool](#)

- [Re: Northwest grounded for 3.5 hours after cable cut](#)

[Henry Spencer](#)

[Bob Dubery](#)

- [Northwest Air fallout: MN backhoe affects FL hotel bookings!](#)

[William Smith](#)

- [Re: MIT grade spreadsheet problem](#)

[Allan Duncan](#)

[Tony Lima](#)

[John Pearson](#)

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

⚡ **More NASA woes in stress testing**

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

Thu, 30 Mar 2000 12:12:19 PST

NASA subjected its \$75M 850-pound High Energy Solar Spectroscopic Imager spacecraft to preflight stress testing, and inadvertently managed to shake it for about 200 milliseconds at 20 (instead of 2) times the force of gravity. Computationally it looks like a small off-by-one error, except that it was one order of magnitude. The HESSI was seriously damaged, with two of its four solar panels cracked. However, it may be salvageable, having continued to function through the testing! [PGN-ed from various sources. It may need HESSian solders to fix it?]

<http://www.abcnews.go.com/sections/science/DailyNews/hessi000323.html>

<http://www.nytimes.com/library/national/science/032400sci-nasa-satellite.html>

[Note: the 2000-pound PC noted in [RISKS-20.85](#) was pounds Sterling. The 850 pounds above is of course weight. English is wonderfully ambiguous. Sorry for the confusion. PGN]

⚡ Re: Faster, cheaper *not* better

"Peter G. Neumann" <neumann@csl.sri.com>
Thu, 30 Mar 2000 12:19:52 PST

One of the problems associated with the hard landing of the Mars Lander is now believed to have been a software flaw: when the landing gear deployed, the software erroneously concluded landing had been achieved and ordered the engines to be shut down prematurely. [See media reports on 29 Mar 2000.] It is once again clear that faster and cheaper are typically not better. Lowest-common-denominator systems are sure-fire candidates for subsequent appearances in RISKS.

Doneel Edelson noted an AP item in **USA Today** on 22 Mar 2000 that discusses some of NASA's problems -- cutting employees too deeply (from 25,000 to 18,500 over 7 years) and losing veteran engineers, failures in communications between technical people and managers, etc. The article also notes that NASA administrator Daniel Goldin contradicted reports that NASA knew of a rocket-engine flaw that resulted in a mission loss.

✦ **More details on the Sea Launch failure ([RISKS-20.84](#))**

Steven Huang <sthuang@hns.com>

Thu, 30 Mar 2000 16:50:30 -0500

According to a report filed by the Associated Press (<http://www.cnn.com/2000/TECH/space/03/30/sealaunchfailure.ap/index.html>),

the investigation is identifying a configuration error, causing "a valve to remain open in the second stage pneumatic system", which is "involved in the operation and steering of the engine, and the loss of pressure would have reduced the performance so much that an onboard automatic flight termination system would have been triggered." The error is blamed on a ground-based system.

Steven Huang, MobileSat, Hughes Network Systems, 11717
Exploration Lane
Germantown, MD 20876 (240) 453-2357

✦ **Stephen King eBook cracked (Re: Pack, [RISKS-20.85](#))**

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

Mon, 27 Mar 2000 16:56:33 PST

Pirated PDF versions of Stephen King's "Riding the Bullet" have been circulating on the Internet since 17 Mar 2000. While many ISPs have forced members to remove the decrypted files, they are still available from a Swiss site, providing stark evidence of security weaknesses in PC-based eBook distribution systems. The episode has irked the companies developing such

systems, who complain that export restrictions have kept them from using more powerful encryption techniques. [Source: "Cracking the Bullet: Hackers Decrypt PDF Version of Stephen King eBook, by Glenn Sanders and Wade Roush, 23 Mar 2000, full text at <http://www.ebooknet.com/story.jsp?id=16711>]

[But as RISKS readers know, strong crypto by itself is not enough.]

✦ California privacy legislation

"Gillmor, Dan" <DGillmor@sjmercury.com>
Tue, 28 Mar 2000 07:14:16 -0800

[We have been warning about identity theft for many years. It is now becoming a criminal art form. The following item is from the IP list of David Farber <farber@cis.upenn.edu>. PGN]

<http://www.mercurycenter.com/svtech/columns/gillmor/docs/dg032800.htm>

NOT too long ago, someone I know well suffered that most modern of crimes, identity theft. A crook got hold of useful information -- including her Social Security number -- and used it to create a fraudulent identity.

The victim discovered the fraud when bills started coming in for things she hadn't bought. Then ``I got letters from lawyers saying they were suing me because I hadn't paid,'' she says. The onus was on her to make things right with credit bureaus, financial institutions and the like -- and the

paperwork was massive.

This kind of outrage is all too common. American businesses are all too casual with our Social Security numbers and other information. Greasing the wheels of commerce has been far, far more important than protecting people's privacy. Law enforcement, meanwhile, believes it has better things to do than investigate, much less prosecute, such crimes.

But you can almost feel privacy gaining strength as a public issue. The Internet Age has opened people's eyes, because people are beginning to see the consequences when all kinds of data ends up in databases that are open to anyone with sufficient cash.

Not many legislators -- federal, state or local -- have grasped the growing public angst until recently. One of several in the California Legislature who understood the issue early is state Sen. Debra Bowen, D-Redondo Beach, who has introduced several bills that would go a long way toward protecting you and me from predatory data practices.

Criminal records in North Carolina

Joe Thompson <kensey@crowley.orion-com.com>

Sun, 26 Mar 2000 20:18:38 -0500 (EST)

Some time ago I sent in an item ([RISKS-20.17](#)) about the new sex offender database in Virginia and how quickly errors were revealed. On a trip this

weekend to the North Carolina Renaissance Faire, I was watching TV the evening I checked in and saw ads for "123nc.com". Apparently North Carolina has gone Virginia one better -- the Website allows visitors to search *all* criminal records in the state of North Carolina. The risks are the same kind but much magnified.

It's also worth noting that this site does *not* appear to be a state government operation. -- Joe

Joe Thompson | <http://www.orion-com.com/~kensey/> spam+@orion-com.com

[Yes, Virginia, there is a sanity clause (bad pun prompted by the famous letter in the *Herald Tribune* many years ago). Virginia was also the first state to pass UCITA, the Uniform Computer Information Transactions Act, a horrendously bad piece of legislation. Incidentally, Maryland has just jumped on what we hope will not become a bandwagon. PGN]

⚡ Judge issues injunction in software reverse-engineering case

"NewsScan" <newsscan@newsscan.com>
Mon, 20 Mar 2000 08:25:03 -0700

A federal judge in Boston has ordered a halt to distribution of the "cphack" software created by two computer hackers by reverse-engineering the commercially distributed "Cyber Patrol" program that allows parents to shield their children from pornography on the Internet. The

judge's order
also applies to any mirror Websites where the program has been
made
available. Peter Junger, a law professor and free speech
advocate, calls
the ruling "a rather horrifying challenge to people's right to
write
software" and to figure out how it works by taking it apart and
examining
it. [*USA Today* 17 Mar 2000; NewsScan Daily, 20 Mar 2000]
<http://www.usatoday.com/life/cyber/tech/cth570.htm>

[Reverse engineering would be effectively outlawed wherever
UCITA (noted
above) passes. PGN]

⚡ Re: Hackers sued by software-filtering company ([RISKS-20.84-85](#))

"Peter G. Neumann" <neumann@csl.sri.com>
Thu, 30 Mar 2000 12:29:33 PST

However, cphack had been *copyleft* under the Free Software
Foundation's GPL
General Public License (<http://www.gnu.org>), which among other
things makes
redistribution unrestricted.

For background, see Judge Harrington's order:

<http://www.politechbot.com/cyberpatrol/final-injunction.html>

Declan McCullagh reportage:

<http://www.wired.com/news/politics/0,1283,35244,00.html>

<http://www.wired.com/news/politics/0,1283,35226,00.html>

<http://www.wired.com/news/politics/0,1283,35216,00.html>

✶ Re: Hackers sued by software-filtering company ([RISKS-20.84-85](#))

"Ross Oliver" <reo@iwi.com>

Wed, 29 Mar 2000 13:58:23 -0800

In [RISKS 20.85](#), Bear Giles writes:

```
>> To a critical mind, several questions scream out:
>> - why are the blacklists encrypted? [...]
>> - how would knowing that a site is on the blacklist permit a
kid
>> to access the blocked site?
```

Jansson and Skala do use the term "encrypted" to describe how CyberPatrol stores its blocklists. However, after reading the technical details, I think the term "compiled" is more accurate. The file format seems to be optimized for space and efficiency of loading and parsing, with obfuscation as only a side effect.

As to the second question, Jansson and Skala flatly state in their essay:

"Now, let's review our goals. First, we want to break the authentication, so let's talk about that." They refer to the authentication for gaining administrative access, which can then be used to bypass the filter. And they proceed to do so, and tell the world how. This is what got CyberPatrol so ticked off. After the excrement hit the ventilating device, they draped themselves in free speech rhetoric and claims of fair use to justify their actions. Had they limited their analysis to the blacklist file format, CyberPatrol might have had much less legal and public relations leverage.

I am not attempting to defend the actions of the filter vendors. However, when dealing with any organization that claims the moral high ground, your credibility can be deeply affected if your actions are perceived to be questionable in any way. This is a common trap for many techno-rebels, especially youthful ones.

It is interesting to note that the major content filter vendors are repositioning themselves toward the business market. This shift could be because businesses have a more money to spend than parents and libraries, and businesses have much more latitude in the workplace to impose arbitrary restrictions.

Ross Oliver <reo@airaffair.com>

✶ German ministry of family et al. and links to porn

Klaus Brunnstein <brunnstein@informatik.uni-hamburg.de>

Wed, 29 Mar 2000 13:47:13 +0200

German tabloids and media discuss links to porno and sex related Websites which could be found on the homepage of the federal ministry of family, elderly people, women and youth. After some public uproar, the Website is closed now. Some media as well as "experts" from parties in the federal parliament tend to assume that these including these links has originated in the ministry itself (which would indeed be a serious case), but almost

nobody is aware about how easy it is to hack unprotected Websites (in the absence of proper auditing, nothing is known how the links developed).

This case demonstrates several serious aspects of risks:

* despite assumptions that information flows into even remote corners of the "global village", German media and politicians are not aware of well-reported previous events where Websites of government and other institutions have been hacked (cases such as DoJ and Website hacking during Kosovo war have been reported via Internet :-)

* awareness of Internet InSecurity and demand for protective action seems to develop only after malevolent experience; in this sense, hacking may be understood as contributing to improved security, whereas the simple way to protect oneself from the beginning (e.g. by presenting ones Webpages by burning it into a CDR or protecting ones site by firewalls or "properly administrating Websites) is unattractively easy.

* Media and politicians approach the "Information Society" in too uncritical manner to observe its inherent InSecurity. In related discussions, I am often told (even by people with good knowledge of some Computer Science area :-), that Internet was founded as military technology, so it must be inherently secure. As contradicting facts are available easily (when searched for), the assumption that Internet is a heaven of Knowledge is hardly justified.

Regrettably, the security community contributes to

misunderstanding risks by
using terms such as "weaknesses" and "exploits" for software
which is
inherently insecure and unsafe: it is NOT a WEAKNESS which is
exploited, but
it is the basic nature that software is INSECURE and UNSAFE - at
any speed
(esp. at GigaBit instructions per second and GigaByte storage
and GigaBaud
:-) Evidently, it is high time for some "Ralph Nader" to rewrite
that famous
book "Unsafe at any speed" (then addressing problems in
automobile
manufacturing) for the carriers of the "Information Society",
especially
including The Internet.

[More on 30 Mar 2000]

The basic assumption that a ministry responsible for protecting
the youth
against illicit information (such as porn-related sites) shall
guarantee, at
least to some degree, the adequacy of the content of its
Websites (including
essential links against direct access to porno sites) proved to
be wrong in
the reported case. Indeed, the ministry's Webpage linked to a
Website which
lead directly (among many hundreds links related to "women
interests") to
Websites such as callboys.

I am glad to admit that Germany has, so far, not publicly
observed any
attack on a federal government Website. So, our federal
government remains
in its innocent status (concerning this aspect :-).

BUT: evidently, Webpage content quality assurance needs
development, esp. on
government level. One interesting risk now moves its head: how
deep shall

link levels be controlled for some sort of "coherence" with (at least: not directly contradicting) the intentions of the owner of the original Website?
Setting aside the argument that addition of links to referenced Websites may practically not be controlled by the administration of the linking Website, responsibility of Website owners should *at least guarantee* that the *first link* does not point directly to Websites which contradict the intentions and interests of the original Website's owner. In critical cases, one may even require that 2nd-level links must also be assured. When it is true that every Website in The Internet may be reached with at most 7 clicks (as some German "experts" publicly argued), then it seems impracticable to control more than 2 link levels.

Moreover, every government Website should contain a disclaimer that the owner of the Website is not responsible for any link at higher levels, and that the owner's responsibility holds only for the day/time given as actual status ("last updated").

Consequently, "netiquette" must not only address responsible behaviour of customers but also for those offering Internet information.

Klaus Brunnstein (March 30,2000)

✶ Privacy problems with HTTP cache-control

Martin Pool <mbp@LINUXCARE.COM>
Wed, 29 Mar 2000 15:19:21 +1000

[Forwarded to RISKS by Lindsay Marshall, from junkbuster-users. PGN]

executive summary

HTTP cache-control headers such as If-Modified-Since allow servers to track individual users in a manner similar to cookies, but with less constraints. This is a problem for user privacy against which browsers currently provide little protection.

problem statement

Alice is browsing the Web; Bob runs a number of otherwise-unrelated Web servers. Alice makes several requests to Bob's servers over time. Bob would like to tie together as many as possible of the requests made by Alice to learn more about Alice's usage patterns and identity: we call this identifying the request chain. Alice would like to access Bob's servers but not give away this information.

existing approaches

cookies

The standard approach for associating user requests across several responses is the HTTP 'Cookie' state-management extension. The Cookie response header allows a server to ask the client to store arbitrary short opaque data, which should be returned for future requests of that server matching particular criteria. Cookies are commonly used to

store per-user form defaults, to manage Web application sessions, and to associate requests between executions of the user agent.

The user agent always has the option to just ignore the Set-Cookie response header, but most implementations default to obeying it to preserve functionality. Cookies can optionally specify an expiry time after which they should no longer be used, that they should persist on disk between client session, or that they should be passed only over transmission-level-secure connections.

The privacy implications of cookies have been [1]extensively discussed, and several problems have been found and recitified in the past. One example of privacy compromise through cookies is the use of cookies attached to banner images downloaded from a central banner server: the same cookie is used within images linked from several servers, and so the user can be tracked as they move around.

other approaches

An obvious means to associate requests is by source IP address. Over the short term this will generally work quite well, as a client is likely to use a single IP address during a browsing session. Even then it is complicated by proxies acting for multiple clients, network address translation, or multiuser machines. Over a longer term, the information is convolved by dynamically-assigned IPs, mobile computers moving between networks, dialup pools and the like. Indeed, cookies

were proposed in large part to allow legitimate stateful applications to cope with the impossibility of uniquely identifying users by IP address.

the meantime exploit

The fundament of the meantime exploit is that the server wishes to `tag' the client with some information that will later be reported back, allowing the server to identify a chain. Cookies are a good approach to this, but their privacy implications are well known and so Bob requires a more surreptitious approach.

The HTTP cache-control headers are perfect for this: the data is provided by the server, stored but not verified by the client, and then provided verbatim back to the server on the next matching request.

Two headers in particular are useful: Last-Modified and ETag. Both are designed to help the client and server negotiate whether to use a cached copy or fetch the resource again.

The general approach of meantime is that rather than using the headers for their intended purpose, Bob's servers will instead send down a unique tag for the client.

Last-Modified is constrained to be a date, and therefore is somewhat inflexible. Nevertheless, the server can reasonably choose any second since the Unix epoch, which allows it to tag on the order of one

billion distinct clients.

ETag allows an arbitrary short string to be stored and passed. It is not so commonly implemented in user agents at the moment, and so not such a good choice.

In both cases the tag will be lost if the client discards the resource from its cache, or if it does not request the exact same resource in the future, or if the request is unconditional. (For example, Netscape sends an unconditional response when the user presses Shift+Reload.) Bob has less control over this than he has with cookies, which can be instructed to persist for an arbitrarily long period.

The date is sent back only for the exact same URL, including any query parameters. By contrast, cookies can be returned for all resources in a site or section of a site. This makes Bob's job a little harder.

Bob therefore should make sure that all pages link to a small common resource: perhaps a one-pixel image. This image is generated by a script that supplies and records a unique timestamp to each client, and records whatever is already present.

For a demonstration, more explanation and details, please see

<http://www.linuxcare.com.au/mbp/meantime/>

Martin Pool, Linuxcare, Inc. Linuxcare.

+61 2 6262 8990 mbp@linuxcare.com, <http://www.linuxcare.com/>

⚡ Re: Northwest grounded for 3.5 hours after cable cut (Dixon, [R-20.85](#))

Henry Spencer <henry@spsystems.net>
Sat, 25 Mar 2000 22:03:26 -0500 (EST)

>When will people learn they need to know where their redundancy lies?
>Cables run through the same conduit are only partially redundant...

Alas, merely wanting the information is not enough. The wire/fiber providers often are not particularly forthcoming with this information; worse, typically it is subject to change without notice. They have deeply-ingrained organizational beliefs that (a) it's nobody's business but theirs where the wires run, and (b) a wire is a wire and which conduit it goes through doesn't matter. If memory serves, even customers whose contracts explicitly called for routing diversity have been bitten by this.

[Virginia, again. Two adjacent fiber cables were severed in Annandale VA on 14 Jun 1991, taking out 80K circuits. I believe that after the White Plains NY ARPAnet cable cut that cut all 7 links to New England, either AP or UPI (or perhaps even both) had insisted that their connections should be in different conduits. The outage affected AP, UPI, and Pentagon, among others. (See [RISKS-11.92](#)). PGN]

✈ **Re: Northwest grounded for 3.5 hours after cable cut (Dixon, [R-20.85](#))**

"Bob Dubery" <bdubery@netcare.co.za>

Sat, 25 Mar 2000 07:13:51 +0200

A recent edition of **New Scientist** carried a short report on an international telecomm conference. One of the interesting points in that report was that Singapore has an enviably low rate of telephone and data cable outages. The reason? If a cable is cut by a building crew then the foreman gets to spend time in jail.

That's draconian. But cables, and the information that they carry, are now so important to businesses, commerce, and, increasingly, to public safety and transport, that contracts should stipulate penalties to be imposed in the case of cable breaks.

The risk of not doing so is becoming increasingly obvious.

✈ **Northwest Air fallout: MN backhoe affects FL hotel bookings!**

"William P. N. Smith" <wpns@compusmiths.com>

Tue, 28 Mar 2000 10:48:18 -0500

From the **Orlando Sentinel** (orlandosentinel.com), Northwest Airlines had to book 50 rooms at the Orlando Airport Hyatt Regency when they lost most of their comm lines recently due to backhoe fade. They didn't say if other Northwest counters had to book hotels in other airports, but I can't imagine

they didn't.

Yet another example of how interconnected things are, how single points of failure you never knew existed can cause havoc, and how we discover those same single points of failure (the hard way). Don't get me started on how tightly scheduled the airlines, airports, and flight crews are, where a few minutes of delay in one flight can ripple through the system and cause innumerable delays for the rest of the day.

William Smith wpns@compusmiths.com N1JBJ@amsat.org
ComputerSmiths Consulting, Inc. www.compusmiths.com

✉ Re: MIT grade spreadsheet problem (Franklin, [RISKS-20.85](#))

Allan Duncan <a.duncan@trl.telstra.com.au>
Mon, 20 Mar 2000 13:05:46 +1100 (EST)

The problem of the spread-sheet sort scrambling data has been around for a while. MS Excel, Office 97 and before can do it, but only recently did I catch it in the act and as a result deduce the trigger.

If you have a spread-sheet with some blank entries in the top row, as may well happen if there is no headings row, then the columns with the blank top elements will not be included in the sort.

There may be other requirements as well, but in the case at hand that was the necessary condition.

⚡ Re: MIT grade spreadsheet problem (Franklin, [RISKS-20.85](#))

Tony Lima <TonyLima@ms.spacebbs.com>

Fri, 24 Mar 2000 18:55:55 -0800

"When the only tool you have is a hammer, every problem looks like a nail."

The real problem here is using spreadsheet software when record integrity is required. That implies use of some sort of decent database program -- which Excel and other spreadsheets are not.

Over the 25 years I've been teaching college, I've experimented with a variety of grading media. On the rare occasions when I teach a class with over 100 students, I use a standard dbf file structure (usually with some version of Foxpro). Otherwise, I use the only tool I've found that meets my criteria of durability, portability and readability: a deck of 3x5 index cards, one card per student. - Tony Lima (professor of economics, Cal. State Hayward)

⚡ Re: MIT grade spreadsheet problem (Franklin, [RISKS-20.85](#))

John Pearson <huiac@camtech.net.au>

Sat, 25 Mar 2000 16:58:09 +1030

Am I alone in thinking that this misses the obvious point that the error arose because the coordinator used a spreadsheet to do a database's job?

[Evidently not. See Tony Lima's message! PGN]

Application vendors have spent considerable effort adding features to word processors and spreadsheets that extend their areas of application, without necessarily improving the usability and reliability of their product; in this case it sounds like vi, sort and awk may have been more reliable candidates for the job.

This specific risk is one I encountered more than once while working in the public sector; at the time it was tolerated because of the huge disparity between the cost and availability of spreadsheets (typically, bundled with your word processor or the PC itself) and database software (several hundred dollars, often with only rudimentary reporting and presentation capabilities).

Are things still that bad, or are people really that resistant to the idea of using the right tool for the job?

[It's as old as the Code of Hammer-Robbie! PGN]

John P. <huiac@camtech.net.au> <john@huiac.apana.org.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 20: Issue 87

Friday 28 April 2000

Contents

- [Explanation for long RISKS hiatus](#)
[PGN](#)
- [UCITA, the Uniform Computer Information Transactions Act](#)
[Bruce Schneier](#)
- [Canadian teen held in Web attacks](#)
[NewsScan](#)
- [Swedish 16-year-old arrested 3 hours after Web attack](#)
[Ulf Lindqvist](#)
- [Teenage hacker stole Gates' credit-card info](#)
[NewsScan](#)
- [Man indicted for vandalizing government computers](#)
[NewsScan](#)
- [Hackers penetrate Gazprom](#)
[Steve Bellovin](#)
- [Security experts discover rogue code in Microsoft software](#)
[NewsScan](#)
- [Encryption code protected by First Amendment](#)
[NewsScan](#)
- [Hackers crack code protecting King e-book](#)
[NewsScan](#)

- [U.S. IT job vacancies approach 1 million mark](#)
[NewsScan](#)
 - [Patent Office revamps Web patent review](#)
[NewsScan](#)
 - [Iridium flames out, literally](#)
[NewsScan](#)
 - [Power failure disrupts National Airport](#)
[Andres Zellweger](#)
 - [Software fault stops 76,000 customers receiving phone calls](#)
[John Kerr](#)
 - [Squirrelcide at San Jose Airport](#)
[Dave Stringer-Calvert](#)
 - [Best new Microsoft bug yet](#)
[Martin Minow](#)
 - [Web server displays admin password on failures](#)
[Bill Janssen](#)
 - [Hotmail wants to know...](#)
[Gillian Richards](#)
 - [no, Virginia](#)
[Danny Burstein](#)
 - [REVIEW: "The Social Life of Information", John Seely Brown/Paul Duguid](#)
[Rob Slade](#)
 - [FORMAL METHODS *ELSEwHeRE* --second CfP](#)
[Tommaso Bolognesi](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Explanation for long RISKS hiatus

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

Thu, 30 Mar 2000 12:12:19 PST

I was in Europe, completely off the net for the first two weeks of April, -- including attending a NATO conference in Brussels on Commercial Off-The-Shelf Products in Defence Applications: The Ruthless Pursuit of

COTS, for which I gave a keynote talk on the challenge of building robust systems and discussing COTS vs nonclosed-source software. The slides can be found at <http://www.csl.sri.com/neumann/> . Since returning, I have been trying to play catch-up, and was able to begin to read the RISKS e-mail only in the past two days.

In this issue, I have tried to make a dent in the huge backlog. I am very grateful that I could rely on NewsScan items that wonderfully captured some of the events that happened in the interim. My profound thanks to John Gehl and Suzanne Douglas, for my being able to repeat their copyrighted items here, with their permission, and apologies to their regular readers who are seeing these items for the second time! But otherwise it would have taken much longer to edit down many of the media reports that are still in the queueueueueueue. PGN

✶ UCITA, the Uniform Computer Information Transactions Act

Bruce Schneier <schneier@counterpane.com>
Mon, 17 Apr 2000 13:30:26 -0500

[From CRYPTO-GRAM, April 15, 2000, with permission]

Virginia Gov. James S. Gilmore III signed the UCITA, and it is now law in Virginia. The Maryland legislature overwhelmingly passed the bill, and it is on its way to become law in that state.

I put this horrible piece of legislation in the Doghouse last month, but it's worth revisiting one portion of the act that particularly affects computer security.

As part of the UCITA, software manufacturers have the right to remotely disable software if the users do not abide by the license agreement. (If they don't pay for the software, for example.) As a computer-security professional, I think this is insane.

What it means is that manufacturers can put a back door into their products. By sending some kind of code over the Internet, they can remotely turn off their products (or, presumably, certain features of their products). The naive conceit here is that only the manufacturer will ever know this disable code, and that hackers will never figure the codes out and post them on the Internet.

This is, of course, ridiculous. Such tools will be written and will be disseminated.

Once these tools are, it will be easy for malicious hackers to disable peoples' computers, just for fun. This kind of hacking will make Back Orifice look mild.

Cryptography can protect against this kind of attack -- the codes could be digitally signed by the manufacturer, and the software wouldn't contain the signature key -- but in order for this to work the entire system has to be implemented perfectly. Given the industry's track record at

implementing cryptography, I don't have high hopes. Putting a back door in software products is just asking for trouble, no matter what kinds of controls you try to put into place.

The UCITA is a bad law, and this is just the most egregious provision. It's wandering around the legislatures of most states. I urge everyone to urge everyone involved not to pass it.

Virginia:

<<http://www.washingtonpost.com/wp-dyn/articles/A6866-2000Mar14.html>>

Maryland:

<<http://www.idg.net/idgns/2000/03/29/UCITAPassesMarylandHouse.shtml>>

Canadian teen held in Web attacks

"NewsScan" <newsscan@newsscan.com>

Wed, 19 Apr 2000 07:53:19 -0700

A 15-year-old Canadian boy has been arrested in connection with the denial-of-service attacks that crippled major Web sites including Yahoo, CNN.com, eBay and Amazon in February. The Montreal-area teenager, who uses "Mafiaboy" as his online moniker, was fingered after investigators were able to trace the attacks to that name by examining the log files of a computer at the University of California-Santa Barbara, one of the servers used in the cyber-assaults. [AP/MSNBC 19 Apr 2000: NewsScan Daily, 19

April 2000

<http://www.msnbc.com/news/396994.asp>

To subscribe or unsubscribe to the TEXT version of NewsScan Daily, send an e-mail message to NewsScan@NewsScan.com with 'subscribe' or 'unsubscribe' in the subject line. To subscribe to our new HTML version of NewsScan Daily, send mail to NewsScan-html@NewsScan.com, with the word 'subscribe' as the subject. (Subscribing to the HTML version won't automatically unsubscribe you from the text version; please unsubscribe yourself as explained above.)

We call our news section "Above The Fold" to honor the tradition of the great "broadsheet" newspapers in which editors must decide which news stories are of such importance that they should be placed "above the fold" on the front page. The NewsScan Credo: Be informative, have fun, and get to the point! See <http://www.newsscan.com/>, and send us mail: John Gehl <gehl@NewsScan.com> and Suzanne Douglas <douglas@NewsScan.com>, or call 770-590-1017.

Copyright 2000. NewsScan Daily (R) is a publication of NewsScan.com Inc.

🔥 Swedish 16-year-old arrested 3 hours after Web attack

Ulf Lindqvist <ulf@csl.sri.com>

Wed, 5 Apr 2000 10:15:07 -0700 (PDT)

>From the Web site of Swedish newspaper *Aftonbladet*, April 5

2000:

When the Web server of The Swedish National Board of Health and Welfare (Socialstyrelsen) was attacked, the system operators called the National Police Computer Crime Squad while the attack was still in progress. The police immediately started tracking the intruder and could get the attacker's home phone number from an ISP. A search warrant was issued and only 3 hours after the attack, police entered the home of the alleged attacker, a 16-year-old boy who was arrested before the eyes of his parents. His computer as well as his parents' computer were seized and, according to the police, records found on the computers links them to attacks on other Web sites in Sweden.

Source:

<http://www.aftonbladet.se/nyheter/0004/05/hacker.html> (in Swedish)

What I personally find noteworthy in this story is how quickly the police reacted and that it could be a sign of the trend to treat computer crimes no differently than "low-tech" crime. When organizations see that it actually helps to call the police in cases like this, maybe they will be less reluctant to do so. The deterrent effect on would-be criminals by likely detection and immediate response should not be underestimated.

Ideally, the risk of fast law enforcement response should only worry attackers, but given the current nature of identification and (lack of) authentication on the Internet, it could also pose a risk to

innocent users
whose systems are attacked and used to attack other systems.

Ulf Lindqvist <ulf@sdl.sri.com> System Design Lab, SRI
International,
Menlo Park CA 94025-3493, USA. Phone +1 650 859-2351 <http://www.sdl.sri.com/>

🔥 Teenage hacker stole Gates' credit-card info

"NewsScan" <newsscan@newsscan.com>
Mon, 27 Mar 2000 08:42:39 -0700

Eighteen-year-old Raphael Gray was arrested on 24 Mar 2000 in Wales on charges of Internet fraud following a joint investigation by the FBI and Welsh police. Gray and an unnamed accomplice had allegedly hacked into nine e-commerce sites, stealing credit card information on 26,000 accounts in the U.S., Canada, Thailand, Japan and Britain. Among the credit cards compromised was one belonging to Microsoft chairman Bill Gates. Gray, who calls himself the "Saint of E-Commerce," said, "I just wanted to prove how insecure these sites are. I have done the honest thing, but I have been ignored." Gray and his accomplice e-mailed the credit card details to NBCi, a subsidiary of the NBC broadcasting group. [Reuters/News.com 26 Mar 2000; NewsScan Daily, 27 Mar 2000]
<http://cnet.com/news/0-1007-200-1590629.html?tag=st.ne.1002.bgif.1007-200-1590629>

✶ Man indicted for vandalizing government computers

"NewsScan" <newsscan@newsscan.com>

Thu, 23 Mar 2000 08:09:12 -0700

Twenty-seven-year-old Max Ray Butler of Berkeley, California, has been indicted on charges of breaking into and causing damage to government computers belonging to such agencies as NASA, the Argonne National Labs, the Brookhaven National Lab, the Marshall Space Center, and various facilities of the Department of Defense. Butler (also known as "Max Vision") has in the past been an FBI source, helping the Bureau solve computer crimes.

[AP/*San Jose Mercury News* 23 Mar 2000; NewsScan Daily, 23 Mar 2000]

<http://www.sjmercury.com/svtech/news/breaking/merc/docs/008604.htm>

✶ Hackers penetrate Gazprom

Steve Bellovin <smb@research.att.com>

Wed, 26 Apr 2000 20:46:00 -0400

The Associated Press reports that hackers, in conjunction with an insider, penetrated computer systems belonging to Gazprom, the Russian gas monopoly.

(<http://www.techserver.com/noframes/story/0,2294,500197283-500270387-501418162-0,00.html>)

(<http://www.techserver.com/noframes/story/0,2294,500197283-500270387-501418162-0,00.html>)

What is especially interesting about this case is that they managed to take control of the system controlling the flow of gas in pipelines,

according to
the Russian Interior Ministry. This makes it one of the few
confirmed
incidents of direct cyberthreats to a country's infrastructure.

--Steve Bellovin

[Based on the 26 Apr 2000 AP item, Keith Rhodes also noted that
including Gazprom case, Russian police registered 852 cases of
computer
crime in Russia in 1999, up twelve-fold from the year before.
PGN]

Security experts discover rogue code in Microsoft software

"NewsScan" <newsscan@newsscan.com>

Fri, 14 Apr 2000 09:10:08 -0700

A three-year-old piece of Microsoft software includes a secret
password that
could be used to gain illegal access to hundreds of thousands of
Web sites,
including site management files that could lead to customers'
credit card
numbers. The code was discovered by two security experts who
found within
the code the following message: "Netscape engineers are
weenies!" Microsoft
is urging customers to delete the file, titled "dvwssr.dll," and
plans to
send out an e-mail bulletin and post a warning on its Web site
describing
the security hole. [AP/*San Jose Mercury News*, 14 Apr 2000
[http://www.sjmercury.com/svtech/news/breaking/ap/docs/4267471.
htm](http://www.sjmercury.com/svtech/news/breaking/ap/docs/4267471.htm); NewsScan
Daily, 14 April 2000]

✶ Encryption code protected by First Amendment

"NewsScan" <newsscan@newsscan.com>

Wed, 05 Apr 2000 08:46:37 -0700

A federal appeals court in Ohio has ruled that encryption software code is protected by the First Amendment because such code is a means of communication between computer programmers. The ruling represents the first time that a federal appellate court has decided software code is protected as free speech, says Raymond Vasvari, legal director of the American Civil Liberties Union: "This is a great day for programmers, computer scientists, and all Americans who believe that privacy and intellectual freedom should be free from government control." The court's decision means a lawsuit filed by Cleveland law professor Peter Junger will be reconsidered. Junger had claimed that the government violated his free-speech rights by requiring export licenses for encryption programs. [*Wall Street Journal*, 5 Apr 2000 <http://interactive.wsj.com/articles/SB954899134353800815.htm>; NewsScan Daily, 5 April 2000]

✶ Hackers crack code protecting King e-book

"NewsScan" <newsscan@newsscan.com>

Fri, 31 Mar 2000 08:24:25 -0700

Computer hackers cracked the software code that was designed to prevent multiple downloads of Stephen King's "Riding the Bullet" novella, confirming

publishers' worries over the dangers inherent in electronic publishing. The e-book's publisher, Simon & Schuster, confirmed that at least two hackers downloaded the software necessary to read the book from Glassbook Inc., one of the Web companies given rights to distribute the book, and managed to break the encryption code that prevented more than one customer from having access to each electronic copy sold. Pirated copies of the book were then distributed to about six Web sites and chat groups. The publisher contacted many of the Internet service providers hosting the sites and had them shut down. "All the publishers are well aware there is no perfect technical solution to this problem," says Glassbook president Len Kawell. "We will do our best with technology; the rest is a matter of patrolling." [*Wall Street Journal*, 31 Mar 2000; NewsScan Daily, 31 March 2000 <http://interactive.wsj.com/articles/SB954465411569087773.htm/t000030180.html>]

🚀 U.S. IT job vacancies approach 1 million mark

"NewsScan" <newsscan@newsscan.com>

Tue, 11 Apr 2000 08:14:53 -0700

U.S. technology companies could be left with more than 800,000 unfilled IT job vacancies this year, according to a study by the Information Technology Association of America, which predicts 843,000 slots for database administrators, programmers, software developers, Web designers, and other IT personnel will go begging due to lack of qualified

applicants. The ITAA results mirror those announced by Silicon.com's Skills Survey 2000, which found that 47% of European companies have open IT positions they cannot fill. Research by IDC indicates that the European labor shortage is about 20% less severe than that of the U.S., but that could change as foreign workers flock to fill U.S. jobs, encouraged by more lenient immigration rules. [Silicon.com 11 Apr 2000 <http://www.silicon.com/> ; NewsScan Daily, 11 April 2000]

✦ Patent Office revamps Web patent review

"NewsScan" <newsscan@newsscan.com>

Wed, 29 Mar 2000 07:58:43 -0700

The U.S. Patent and Trademark Office is overhauling the way it reviews applications for many online practices, and will now require a broader search of past practices and inventions before awarding patents. The change comes in response to critics who charge the Office with granting overly broad patents for basic Web techniques, such as Amazon's "1-Click" ordering process. Examiners reviewing applications in the business-method area will now have to follow new procedures, including searching online databases for similar technology ideas. "If you make these decisions without adequate data, you run the very real risk of issuing patents on things that were already invented, or patents that are far broader than they should be," says

Roland Cole, executive director of the Software Patent Institute. [*Wall Street Journal, 29 Mar 2000; NewsScan Daily, 29 Mar 2000]
<http://interactive.wsj.com/articles/SB954286078412266261.htm>

[It's about time. Many patents have been getting through where prior art has been known for years. But it does provide lots of employment for lawyers. PGN]

✶ Iridium flames out, literally

"NewsScan" <newsscan@newsscan.com>
Tue, 11 Apr 2000 08:14:53 -0700

Iridium, the bankrupt global satellite telephone corporation that spent \$5 billion on the creation of a communications system for "anyone, anytime, virtually anywhere in the world," will soon start sending 88 giant satellites hurtling from the skies and burning up before they reach Earth. Noting that the expensive Iridium phones could not even be used indoors, industry-watcher and financial analyst James Grant says, "It was a technology that didn't live up to its hype or its billing. People chose to overlook the risks because they were bedazzled by the technology and the promoters or sponsors." [*The New York Times*, 11 Apr 2000
<http://www.nytimes.com/library/tech/00/04/biztech/articles/11iridium.html>;
NewsScan Daily, 11 April 2000]

✶ Power failure disrupts National Airport

Andres Zellweger <ZellwegA@cts.db.erau.edu>

Thu, 13 Apr 2000 08:16:07 -0400

At 7:50pm on the evening of 10 Apr 2000, a power failure shut down radar at Washington DC's Reagan National Airport after the backup generator failed at 8:41pm. Traffic was obviously affected. Hotels were full, trying to take care of stranded passengers. [Source: Article by Phuong Ly, *The Washington Post*, 11 Apr 2000, B02]

[Power was resumed around 4am. So much for back-up systems! Dres]

[Yes, they needed backup to the backup.

This event also reported to RISKS by Sy Goodman. PGN]

✶ Software fault stops 76,000 customers receiving phone calls

"John Kerr" <jkerr@gil.com.au>

Thu, 6 Apr 2000 18:04:18 +1000

At 1615 on 6 April 2000 local time, a Telstra spokesman on ABC Public Radio advised that 76,000 telephone customers in the Toowong area of Brisbane, Australia had been affected by a software fault which prevented them receiving incoming calls although he indicated they seemed to be able to ring out. He stated the problem had occurred two hours previously and expected that service would be restored within half an hour but otherwise gave no details. The radio and station [and I] were in the affected area.

John Kerr, jkerr@gil.com.au - St Lucia Brisbane Australia
61 7 3870 9588 when it takes calls

⚡ Squirrelcide at San Jose Airport

Dave Stringer-Calvert <dave_sc@csl.sri.com>

Fri, 14 Apr 2000 06:57:15 -0700

Squirrel cuts power to airport [From www.newschannel11.com]

A spokesman for Pacific Gas & Electric said power was restored to Santa

Clara County office buildings and the San Jose International Airport and all

other customers around 2:30pm. ... 1,300 customers lost power around noon

when a squirrel touched a conductor and blew a circuit breaker.

As power

failed, back-up generators kept the airport running and planes continued to

take off and land on time. ... No flight delays ... No traffic lights

around the airport... luggage handled by hand ... Terminal C only. [PGN-ed]

⚡ Best new Microsoft bug yet

"Martin Minow" <martin.minow@thinklinkinc.com>

Tue, 18 Apr 2000 13:26:39 -0700

<http://support.microsoft.com/support/kb/articles/Q131/1/09.asp>

Explorapedia Nature: Earth Rotates in Wrong Direction

The information in this article applies to:

Microsoft Explorapedia series: World of Nature for Windows,

version 1.0

SUMMARY

When you run Explorapedia and use the Exploratron to look at the Earth spinning, the Earth rotates in the wrong direction.

STATUS

Microsoft has confirmed this to be a problem in Explorapedia, World of Nature, version 1.0. We are researching this problem and will post new information here in the Microsoft Knowledge Base as it becomes available.

[Transcribed by Martin Minow, minow@pobox.com
(I shouldn't be so smug, as I got this wrong in one of my applets, too.)]

🔥 Web server displays admin password on failures

Bill Janssen <janssen@parc.xerox.com>

Wed, 23 Feb 2000 18:44:04 PST

Here's a classic from the pilot-unix mailing list:

```
Subject: [Pilot-Unix] Palm Store
From: Justin Osborn <josborn@mbhs.edu>
Date: Wed, 23 Feb 2000 18:04:44 PST
To: mblug@mbhs.edu, Palm Unix List <pilot-unix@hccirisc.cs.
binghamton.edu>
```

I went to the Palm Store (palmorder.modusmedia.com) and I did a search for

"Minstrel." I got this error message:

```
CGI Error
```

```
The specified CGI application misbehaved by not returning a
complete set
```

```
of HTTP headers. The headers it did return are:
```

Died at D:\enGarde\Apps\Palm\cgi-bin\palmsearch.cgi line 63.
dsn=palm;SERVER=ecom-websql;UID=sa;PWD=[***** deleted for
RISKS by PGN]

----- Error Report:-----

Errors for the package: Connection Number: Error number:
1326

Error message: "[Microsoft][ODBC SQL Server Driver]Client
unable to
establish connection"

[...] Displaying the system admin password? Come on...

Justin Osborn

Bill Janssen <janssen@parc.xerox.com> (650) 812-4763 FAX:
(650) 812-4777

Xerox Palo Alto Research Center, 3333 Coyote Hill Rd, Palo Alto,
CA 94304

🔥 Hotmail wants to know...

"Richards, Gillian" <gillian.richards@tafensw.edu.au>

Thu, 27 Apr 2000 10:50:45 +1000

A friend (and indeed myself) write characters in assorted
newsgroups, and
not all the characters are human. To keep mail pertaining to
those
characters separate from work, etc, we created Hotmail accounts
for each
character, and filled in the statistics as if it were the
character. As an
example, I write a rabbit who is aged about 18 months - the
equivalent of a
young adult in human terms. (If any of the other writers are
reading this, I
deny being any of them {fluffystomp!})

Now Hotmail won't let us access our accounts as we are "underaged", unless an adult verifies that we are allowed to.

The proof of adult status required? A credit card number.

The risks:

1) I refuse to give my credit card number for a non-purchase reason.

2) Who says a real kid is going to enter their correct age anyway?

(just like the "click here if you are over 18" checks of the adult sites)

3) If we put in our real ages (and indeed our real details such as

zip/post codes and other such stuff) just how much free marketing

information is Hotmail getting out of us?

Hotmail can trace any mail back to my own ISP account if necessary. Surely

that's more than enough information for them. If I start getting junk mail

in my ISP mailbox for rabbit feed and viagra, I'll know why.

Gillian the Techie

🔥 no, Virginia (Re: [RISKS-20.86](#))

danny burstein <dannyb@panix.com>

Fri, 31 Mar 2000 12:07:19 -0800 (PST)

Permit me to point out that the famous letter, from Virginia O'Hanlon, was

first printed in the **New York Sun** of 21 September 1897.

[TNX. For historical accuracy, not RISKS relevance. PGN]

✦ REVIEW: "The Social Life of Information", John Seely Brown/ Paul Duguid

"Rob Slade" <rslade@sprint.ca>
Tue, 18 Apr 2000 08:11:42 -0800

BKSOLFIN.RVW 20000222

"The Social Life of Information", John Seely Brown/Paul Duguid,
2000,

0-87584-762-5, U\$25.95

%A John Seely Brown jsb@parc.xerox.com

%A Paul Duguid duguid@socrates.berkeley.edu

%C 60 Harvard Way, Boston MA 02163

%D 2000

%G 0-87584-762-5

%I Harvard Business School Press

%O U\$25.95 800-545-7685 fax: 617-496-8066 www.hbsp.harvard.edu

%P 320 p.

%T "The Social Life of Information"

The book is not very clear about the social life of information, or why we should care about it. For example, the introduction notes that digital communications removes clues that we would ordinarily receive in a conversation, conveyed through body language. It also asserts that there are a number of people involved in the infrastructure behind accessing a piece of printed information, such as publishers and librarians. The irony of these statements seems to be lost: books hide body language just as effectively as e-mail, and the Internet is the product of a number of

communities of people, the cultures of whom are apparent to those who choose to examine the net closely.

Chapter one examines the information glut, as well as touching on the fact that knowledge may lose its value as it is atomized into mere data.

However, it is difficult to find any central theme, other than a reaction

against some of the more facile assertions that are being made about the information age. Agent technology and other forms of low level artificial

intelligence are noted to be imperfect, in chapter two.

Starting with

telecommuting, chapter three looks at other aspects of computers and work.

Chapter four discusses the failure of business process re-engineering and

the triumph of informal practices of work and socialization. (I can fully

agree with the comments on the business-term-du-jour.) Social factors

involved in knowledge and learning are addressed in chapter five. A "seed

in good soil" model of technical development structures the presentation of

knowledge ecologies in chapter six. Chapter seven seems to feel that there

is some inherent validation of printed knowledge, but I can certainly attest

to the fact that a lot of books are a waste of good pulp.

Chapter eight

finishes off with a look at higher education, and also provides the only

solid suggestion of the work--the "distributed" college, with separation of

the various functions.

The book makes one important point; that trying to remove information from

its social context is fraught with peril. The text is readable,

and the material is erudite and even, at times, insightful. Unfortunately, this single message, and a bit of tutting at those leaping into digital waters without looking, doesn't seem to be able to carry interest in the volume all the way through. The content is neither new, nor presented in any novel way. Questions or intents are not very clear, nor strongly pursued. The result is probably worth reading as a reminder not to get too caught up in the techno-hype, but is not earth-shaking.

copyright Robert M. Slade, 2000 BKSOLFIN.RVW 20000222
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

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

✶ FORMAL METHODS *ELSEwHeRE* --second CfP

Tommaso Bolognesi <t.bolognesi@IEL.PI.CNR.IT>

Fri, 21 Apr 2000 16:21:30 +0100

F M - E L S E w H e R E (F O R M A L M E T H O D S * E L S E W H E R E *)
A Satellite Workshop of FORTE-PSTV-2000,
devoted to applications of Formal Methods to areas
other than communication protocols and software
engineering.

P i s a , I t a l y , O c t o b e r 1 0 , 2 0 0 0

FM-ELSEWHERE Web page

<http://www.cs.ukc.ac.uk/people/staff/hb5/Elsewhere/>

FORTE/PSTV Web page

<http://forte-pstv-2000.cpr.it>

... Also, we will be keeping a list of known non-traditional

applications of

formal methods on the workshop web page,

<http://www.cs.ukc.ac.uk/people/staff/hb5/Elsewhere/>

and if you wish to contribute an item to the list mail Howard Bowman

(H.Bowman@ukc.ac.uk).

SUBMISSIONS by 15 May 2000

Send by e-mail a copy of your paper to Howard Bowman (H.Bowman@ukc.ac.uk).



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 88

Sunday 14 May 2000

Contents

- [Love Letter Worm, CERT Advisory CA-2000-04](#)
[CERT](#)
- [Mainstream media get a clue about Microsoft security](#)
[Russ Cage](#)
- [Peacefire: Eudora "Stealth Attachment" Security Hole Discovered](#)
[Bennett Haselton](#)
- [Netscape Navigator Improperly Validates SSL Sessions, CERT Advisory CA-2000-05](#)
[CERT](#)
- [FBI gun-check computer crashes](#)
[Declan McCullagh](#)
- [Risk: Selective denial of GPS signals](#)
[Mike Fisk](#)
- [Phone fault sparks sausage frenzy](#)
[Ian Simpson](#)
- [Network trashcan](#)
[Conrad Heiney](#)
- [Stupid appliance ideas](#)
[Lloyd Wood](#)
- [netzero: defenders of the free world?](#)
[Laurentiu Badea](#)

- [Re: Security experts discover rogue code in Microsoft software](#)
[Russ Cooper](#)
 - [Re: Encryption code protected by First Amendment](#)
[Terry Carroll](#)
 - [Re: Hotmail wants to know...](#)
[Jon Ribbens](#)
 - [Re: No, Virginia](#)
[Mark Brader](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Love Letter Worm, CERT Advisory CA-2000-04

CERT Advisory <cert-advisory@cert.org>

Thu, 4 May 2000 20:43:48 -0400 (EDT)

[Always check the CERT Web site for updates on any CERT Advisory that is included in RISKS. This item is a starkly abridged version of the original Advisory 2000-04. Subsequent to the first appearance of ILOVEYOU, there have been numerous copycat variants, and assessments of damage on the order of many billion dollars.]

[HOWEVER, please take a look at my written testimony on ILOVEYOU and its wider implications, which I submitted to the House Science Committee Subcommittee on Technology on 10 May 2000, Risks in Our Infrastructures: The Tip of a Titanic Iceberg Is Still All That Is Visible --

<http://www.csl.sri.com/neumann/house00.html>

PGN]

CERT Advisory CA-2000-04 Love Letter Worm

Original release date: May 4, 2000

Last revised: --

Source: CERT/CC

Systems Affected

* Systems running Microsoft Windows with Windows Scripting Host enabled

Overview

The "Love Letter" worm is a malicious VBScript program which spreads

in a variety of ways. As of 2:00pm EDT(GMT-4) May 4, 2000 -- the CERT

Coordination Center has received reports from more than 250 individual

sites indicating more than 300,000 individual systems are affected. In

addition, we have several reports of sites suffering considerable

network degradation as a result of mail, file, and web traffic generated by the "Love Letter" worm.

I. Description

You can be infected with the "Love Letter" worm in a variety of ways,

including electronic mail, Windows file sharing, IRC, USENET news and

possibly via webpages. Once the worm has executed on your system, it

will take the actions described in the Impact section.

Electronic Mail

When the worm executes, it attempts to send copies of itself using

Microsoft Outlook to all the entries in all the address books. The

mail it sends has the following characteristics:

- * An attachment named "LOVE-LETTER-FOR-YOU.TXT.VBS"
- * A subject of "ILOVEYOU"
- * A body which reads "kindly check the attached LOVELETTER

coming
from me."

People who receive copies of the worm via electronic mail will most likely recognize the sender. We encourage people to avoid executing code, including VBScripts, received through electronic mail regardless of the sender without firsthand prior knowledge of the origin of the code.

Internet Relay Chat

When the worm executes, it will attempt to create a file named script.ini in any directory that contains certain files associated with the popular IRC client mIRC. The script file will attempt to send a copy of the worm via DCC to other people in any IRC channel joined by the victim. We encourage people to disable automatic reception of files via DCC in any IRC client.

Executing Files on Shared File Systems

When the worm executes, it will search for certain types of files and replace them with a copy of the worm (see the Impact section for more details). Executing (double clicking) files modified by other infected users will result in executing the worm. Files modified by the worm may also be started automatically, for example from a startup script.

Reading USENET News

There have been reports of the worm appearing in USENET newsgroups.

The suggestions above should be applied to users reading messages in USENET newsgroups.

II. Impact

When the worm is executed, it takes the following steps:

Replaces Files with Copies of the Worm

When the worm executes, it will search for certain types of files and

make changes to those files depending on the type of file.

For files

on fixed or network drives, it will take the following steps:

* For files whose extension is vbs or vbe it will replace those

files with a copy of itself.

* For files whose extensions are js, jse, css, wsh, sct, or hta, it

will replace those files with a copy of itself and change the

extension to vbs. For example, a file named x.css will be replaced

with a file named x.vbs containing a copy of the worm.

* For files whose extension is jpg or jpeg, it will replace those

files with a copy of the worm and add a vbs extension. For example, a file named x.jpg will be replaced by a file called

x.jpg.vbs containing a copy of the worm.

* For files whose extension is mp3 or mp2, it will create a copy of

itself in a file named with a vbs extension in the same manner as

for a jpg file. The original file is preserved, but its attributes

are changed to hidden.

Since the modified files are overwritten by the worm code rather than

being deleted, file recovery is difficult and may be impossible.

Users executing files that have been modified in this step will cause the worm to begin executing again. If these files are on a filesystem shared over a local area network, new users may be affected.

Creates an mIRC Script

While the worm is examining files as described in the previous section, it may take additional steps to create a mIRC script file. If the file name being examined is mirc32.exe, mlink32.exe, mirc.ini, script.ini or mirc.hlp, the worm will create a file named script.ini in the same folder. The script.ini file will contain:

```
[script]
```

```
n0=on 1:JOIN:#:{
n1=  /if ( $nick == $me ) { halt }
n2=  /.dcc send $nick DIRSYSTEM\LOVE-LETTER-FOR-YOU.HTM
n3=}
```

where DIRSYSTEM varies based on the platform where the worm is executed. If the file script.ini already exists, no changes occur.

This code appears to define a script such that whenever the user joins a channel in IRC, a copy of the worm will be sent to others on the channel via DCC. The script.ini file is created only once per folder processed by the worm.

Modifies the Internet Explorer Start Page

If the file <DIRSYSTEM>\WinFAT32.exe exists, the worm sets the Internet Explorer Start page to one of four randomly selected URLs.

These URLs all refer to a file named WIN-BUGSFIX.exe, which

presumably

contains malicious code. The worm checks for this file in the Internet Explorer

downloads directory, and if found, it is added to the list of

programs to run at reboot. The Internet Explorer Start page is then

reset to "about:blank". Information about the impact of running

WIN-BUGSFIX.exe will be added to this document as soon as it is available.

Send Copies of Itself via E-mail

The worm will attempt to use Microsoft Outlook to send copies of itself to all entries in all address books as described in the Description section.

Other Modified Registry Keys

In addition to other changes, the worm updates the following registry keys:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel32
HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
\Win32DLL
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WIN-BUGSFIX
HKCU\Software\Microsoft\Windows Scripting Host\Settings
\Timeout
HKCU\Software\Microsoft\Internet Explorer\Main\Start Page
HKCU\Software\Microsoft\WAB\*
```

III. Solution

- Update Your Anti-Virus Product [...]
- Disable Windows Scripting Host [...]
- Disable Active Scripting in Internet Explorer [...]
- Disable Auto-DCC Reception in IRC Clients [...]
- Filter Virus in E-Mail [...]
- Sendmail [...]

PostFix [...]
Procmail [...]
Exercise Caution When Opening Attachments [...]
Appendix A. Anti-Virus Vendor Information [...]

[The full Advisory as updated is available from:
<http://www.cert.org/advisories/CA-2000-04.html>]

CERT/CC Contact Information

E-mail: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT personnel answer the hotline 08:00-20:00 EST(GMT-5) / EDT
(GMT-4)

Monday through Friday; they are on call for emergencies
during other
hours, on U.S. holidays, and on weekends.

Conditions for use, disclaimers, and sponsorship information
[...]

Copyright 2000 Carnegie Mellon University.

[PGN-ed for RISKS.]

⚡ Mainstream media get a clue about Microsoft security

Russ Cage <spherethis@yahoo.com>
Fri, 5 May 2000 10:01:20 -0700 (PDT)

In the flurry of news about the LoveBug virus, this article
stands out:

http://news.bbc.co.uk/low/english/sci/tech/newsid_737000/737396.stm.

It represents one of the first mainstream media pieces to note that the problem with computer viruses is enabled by Microsoft's designs and wouldn't exist without them.

``Peter Sommer... told BBC News Online that Microsoft created these by building in to their software the tools needed to customize applications. Microsoft customers are going to have to ask the company to review very carefully the level of functionality that they are putting into their systems. [...] One has got to ask why products are put out which contain these programming languages, which may be of use to perhaps only 3 to 4% of the customers but for everyone else presents a considerable threat. [...] These features are also very difficult to turn off. The lesson from Love Bug is that people must be able to kill off this programming functionality within applications programs."

Other experts from virus companies are quoted as deflecting the blame from Microsoft, but their business interests depend on there being viruses to stop. If the Windows security model made it very difficult for viruses to propagate, these companies would probably not exist any more.

Peacefire: Eudora "Stealth Attachment" Security Hole Discovered

Bennett Haselton <bennett@peacefire.org>

Thu, 27 Apr 2000 18:35:39 -0500

Peacefire has discovered a security hole in all versions of Eudora mail for Windows, that can allow a hacker to execute code on a user's machine, by sending the user e-mail and having them click on a link:

<http://www.peacefire.org/security/stealthattach/>

(For example, a Eudora user would see this message with the URL above made into a hyperlink so that you can click on it and load it into your browser. Using the "stealth attachment" security exploit, you can force code to run on the user's machine when they click on the link. Don't worry, **this** message is safe :-) But you can go to the above URL and request a "demonstration mail" to be sent to you.)

Security holes that allow you to run code on a remote user's machine just by sending them e-mail, are extremely dangerous -- a hacker could use this to steal or erase any classified data on a remote user's hard drive, even if that user were behind a corporate firewall and had anti-virus software running. A virus writer could use the exploit to write a virus that could spread to almost all Eudora users -- numbering in the millions -- and potentially do hundreds of millions of dollars' worth of damage. (Unlike most such tricks, this exploit does not require the user to do anything "naive", like run an .exe that is sent to them as an attachment.) USA Today reported last year on the "BubbleBoy" virus, which similarly used a security hole in Microsoft Outlook to cause code to run on a user's

machine, simply

by reading an e-mail message:

<http://www.usatoday.com/life/cyber/tech/ctg633.htm>

Unfortunately, unlike the security hole that Peacefire discovered last week:

<http://www.peacefire.org/security/jscookies/>

<http://news.cnet.com/news/0-1005-200-1717169.html>

<http://www.zdnet.com/zdnn/stories/news/0,4586,2553337,00.html>

<http://www.ntsecurity.net/go/load.asp?id=/security/netscape2.htm>

this security hole doesn't involve any cool industry buzzwords like

"javascript" or "cookies". This one just involves -- *YAWN* -- e-mail. That is, like, *so* 20th-century. Sorry if this is inconvenient

for journalists writing about this stuff :-)

bennett@peacefire.org

(425) 649 9024

<http://www.>

[peacefire.org](http://www.peacefire.org)

⚡ Netscape Navigator Improperly Validates SSL Sessions, CERT Advisory CA-2000-05

CERT Advisory <cert-advisory@cert.org>

Fri, 12 May 2000 15:06:11 -0400 (EDT)

CERT Advisory CA-2000-05

Netscape Navigator Improperly Validates SSL Sessions

Original release date: May 12, 2000

Source: ACROS, CERT/CC [...]

Systems Affected

* Systems running Netscape Navigator 4.72, 4.61, and 4.07.

Other

versions less than 4.72 are likely to be affected as well.

Overview

The ACROS Security Team of Slovenia has discovered a flaw in the way

Netscape Navigator validates SSL sessions.

[The complete CERT Advisory is available from:

<http://www.cert.org/advisories/CA-2000-05.html>

PGN-ed for RISKS]

FBI gun-check computer crashes

Declan McCullagh <declan@well.com>

Sat, 13 May 2000 11:51:37 -0400

<http://www.wired.com/news/print/0,1294,36310,00.html>

The FBI's Interstate Identification Index database system crashed on 11 May, preventing background checks of some 100,000 would-be gun purchasers who have to be vetted by the National Instant Check System. The crash also prevented use of the Integrated Automated Fingerprint Identification System associated with the National Crime Information Center NCIC 2000. Service expected to return on 14 May. [The U.S. General Accounting Office notes that NICS was offline for 215 hours from November 1998 to November 1999. [PGN-ed]

✦ Risk: Selective denial of GPS signals

Mike Fisk <mfisk@lanl.gov>

Mon, 1 May 2000 17:44:03 +0000 (GMT)

President Clinton announced today that the US government will no longer use its "Selective Availability" feature to degrade the precision of measurements possible with civilian (and non-US government) Global Positioning System (GPS) receivers. One of the concerns cited in the announcement is the ability to use GPS for emergency response and other critical, civilian uses.

It is also stated that one of the reasons the US is comfortable making this change is that it has "demonstrated the capability to selectively deny GPS signals on a regional basis when our national security is threatened."

The risks: Will this lead to more dependence on a system that may be made unavailable at any time? For example pilots, outdoor enthusiasts, and rescue services all use GPS for routine navigation. If that signal was suddenly made unavailable, would these people still have the necessary skills to navigate using non-GPS techniques such as map and compass and terrestrial radio beacons? What about fail-over in automatic computer systems (such as autopilots) that depend on GPS?

The full announcement is available at the following URL:

<http://www.igeb.gov/sa/potus.txt>

Mike Fisk, RADIANT Team, Network Engineering Group, Los Alamos National Lab

See <http://home.lanl.gov/mfisk/> for contact information

⚡ Phone fault sparks sausage frenzy

"Ian Simpson" <ian.g.simpson@btinternet.com>

Thu, 4 May 2000 18:54:25 +0100

Alison Mckenzie, of Peterhead, in Aberdeenshire, phoned a 24-hour environmental services helpline after a chorizo sausage she had bought turned out to be green. As a result of a British Telecom system fault, the call was automatically forwarded to police service voicebanks, but also in text form to every BT pager number beginning with 01426.

[Not green with envy, and certainly not environmentally green.

Mayhaps it was an Irish chorizo? As usual, the wurst is yet to come.

PGN-ed from Ian's sources,

<http://news2.thls.bbc.co.uk/hi/english/uk/scotland/newsid%5F735000/735531.stm>

<http://www.thisisnorthscotland.co.uk/scripts/edarticle-p.asp?section=National+news&ID=29726&source=NAT>]

⚡ Network trashcan

"Conrad Heiney" <conrad@fringehead.org>

Fri, 28 Apr 2000 15:22:28 -0700

A friend of mine works for [Huge Corporation], where security is frequently announced as being imperative. The operating system of choice is Windows NT, and much work is shared on a networked "drive" type share. This "drive" has

a trashcan icon on it.

Fishing in said network trashcan results in the discovery of all sorts of information, including Word documents with draft policies, the home addresses of top executives, financial information, etc.

The RISK here is that people expect something that looks like a trashcan to behave like one, and behave accordingly. The Memory Hole has become a security hole.

-- Conrad Heiney conrad@fringehead.org <http://fringehead.org/>

[Ah, yes, that is just like your home trashcans. Publically available. You have no idea what dumpster diving can go on after you put something in it. Don't forget all the deleted stuff

still in the Word file. You need a bit shredder.

Cryptography?

Still maybe not enough, but closer. PGN]

✶ Stupid appliance ideas

Lloyd Wood <l.wood@eim.surrey.ac.uk>

Sun, 7 May 2000 00:32:36 +0100 (BST)

Of late, there has been a surge in interest in networking domestic appliances. Electrolux and Whirlpool plan ScreenFridges, where you can see recipes and order food. Ariston has a washing machine with a built-in modem which can telephone automatically for software upgrades for the programme controller.

And now there's BT, with:

<http://www.telegraph.co.uk/et?ac=000111464113065&pg=/et/00/5/7/ntac07.html>

where domestic appliances are chipped and authorised for use by a home management centre phoning your insurance company.

The failure modes here are legion. Move house, and discover that your appliances no longer work while you enter a protracted discussion with your insurance company to authorise your home management centre in its new location (no doubt necessary to prevent the home management centre from being stolen). Have your home management centre crash [Ariston has proposed its kitchen centre be run on Windows CE], and watch it take out your entire kitchen, denying you service in the process.

Not so much white goods ideas, as white jacket ideas. It's a recipe for disaster.

plumb and play. hah.

<L.Wood@surrey.ac.uk>PGP<<http://www.ee.surrey.ac.uk/Personal/L.Wood/>>

netzero: defenders of the free world?

Laurentiu Badea <bytemare@lmm.pub.ro>
29 Apr 2000 17:19:10 -0700

The "Terms and Conditions" you must accept to use the "free" NetZero service include giving up your privacy among other "minor" things:

- 1) obligation on your part to fill out with real information all questionnaires and survey forms they send;
- 2) allowing NetZero to learn your browsing habits by tracking all the websites you visit and compile, sell and USE that information. They say personal identifying info won't be disclosed but just the simple fact that they store it on their system where is available to anybody who could lawfully or not access it, is a problem. Let alone they don't exclude themselves from using it so it is possible for them to target you directly.
- 3) you cannot disable cookies, bypass their ad program (meaning that you can't install firewalling software that would block the ad stream)
- 4) you allow them to alter your e-mail messages by adding advertising which you cannot remove or obscure (not unusual);
- 5) the most ridiculous note is that the whole agreement can be changed at any time by posting them on their website, and require you to check them every time before you "use the service", and not use it if you don't agree. Let alone the impossibility of this (how can you browse their website without already being connected, thus using the service), it puts an unreasonable burden on the user. How many will remember the original contract and check the new one for differences, I doubt they would post a "diff" file there :-)

Laurentiu Badea

⚡ Re: Security experts discover rogue code in Microsoft software

Russ <Russ.Cooper@rc.on.ca>

Mon, 1 May 2000 08:51:05 -0400

It's extremely important to clarify this "Netscape engineers are weenies!" story.

For a variety of reasons, one of which being my own quotes in the original *Wall Street Journal* article on this issue, the public has been overly warned against an extremely limited threat... while the real threat from the `dvwssr.dll` has been largely ignored by the media.

First, clarification of the "secret backdoor password" threat. The possibility that the string above could be used to access the source of Active Server Page (.asp) web files, or configuration files known as .asa, is entirely dependent on the permissions configured on an IIS web server. By default, no access can be gained. If permissions are mis-configured, allowing anonymous read access to the files (they should be permissioned for anonymous *execute*, not read), then there is a way that the obfuscation could permit access. It should be noted that with such a mis-configured system, numerous other access methods would be available also.

The important story overlooked was a discovery by CORE-SDI later in the evening after the backdoor story had run virtually everywhere.

CORE-SDI, not more than 8 hours after first looking at the `dvwssr.dll`, was able to published details on a buffer overrun in that .dll that could permit

a DoS of IIS boxes. By some other machinations (including moving the file to a directory where it would not normally be found), they were able to execute arbitrary code on the attacked box.

Everyone, RFP (who's advisory caused the original stir), CORE-SDI, and Microsoft advised that the dvwssr.dll simply be deleted (from all of its locations) in order to remedy the potential problem(s).

While this particular program had minimal use in its lifetime, the fact that a static password (used for obfuscation, not entry) was even present should not be understated. This program has survived numerous Q&A cycles and, if we believe that source code for NT has been available at some 30+ U. S. Universities for years, numerous code reviews.

Of interest to RISKS readers should be the fact that MS was, presumably, unaware that it was using obfuscation for security in that program.

Russ - NTBugtraq Editor
"dot-age" (as in "we're in the dot-age") = senility (source Webster's)

⚡ Re: Encryption code protected by First Amendment

Terry Carroll <carroll@tjc.com>
Fri, 28 Apr 2000 19:57:23 -0700 (PDT)

On Wed, 05 Apr 2000, "NewsScan" wrote:

> A federal appeals court in Ohio has ruled that encryption

software code is
> protected by the First Amendment because such code is a means
of
> communication between computer programmers.

For those who want to read the court's opinion itself, it's
online at
the Sixth Circuit Court of Appeals website. The URL is
<[http://pacer.ca6.uscourts.gov/cgi-bin/getopn.pl?
OPINION=00a0117p.06](http://pacer.ca6.uscourts.gov/cgi-bin/getopn.pl?OPINION=00a0117p.06)>; a
PDF-formatted file (in two-up form intended for publication as a
slip
opinion, so the pagination may look odd to you) is at
<<http://pacer.ca6.uscourts.gov/opinions.pdf/00a0117p-06.pdf>>.

The citation is *Junger v. Daley*, No. 98-4045 (6th Cir. Apr. 4,
2000).

The opinion is only 8 pages long, most of which simply relates
the facts,
discusses the standard of appellate review, or states the
restates resulting
order. The analysis of source code as speech is remarkably
short, on page
7, the gist of which is:

The Supreme Court has expressed the versatile scope of the
First
Amendment by labeling as "unquestionably shielded" the artwork
of
Jackson Pollack, the music of Arnold Schoenberg, or the
Jabberwocky
verse of Lewis Carroll. ... Though unquestionably expressive,
these
things identified by the Court are not traditional speech.
Particularly, a musical score cannot be read by the majority
of the
public but can be used as a means of communication among
musicians.
Likewise, computer source code, though unintelligible to many,
is the
preferred method of communication among computer programers
[sic].

Because computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment.

Terry Carroll, Santa Clara, CA <carroll@tjc.com> "The United States is located in the District of Columbia." Uniform Commercial Code s. 9-307(h)

✉ Re: Hotmail wants to know... (Richards, [RISKS-20.87](#))

Jon Ribbens <jon@oaktree.co.uk>
Mon, 1 May 2000 20:28:41 +0100

>The proof of adult status required? A credit card number.
>1) I refuse to give my credit card number for a non-purchase reason.

You may well find that your credit card Terms and Conditions forbid you from giving your credit-card number to anyone for any reason other than making a purchase. Mine do.

Jon Ribbens / jon@oaktree.co.uk

✉ Re: No, Virginia (Burstein, [RISKS-20.86](#))

Mark Brader <msb@vex.net>
Fri, 28 Apr 2000 21:21:59 -0400 (EDT)

Danny Burstein writes:

> Permit me to point out that the famous letter, from Virginia

O'Hanlon, was
> first printed in the *New York Sun* of 21 September 1897.

And in the letter, Virginia quotes her father as saying "if you see it in the Sun, it's so".

The New York Sun is also the paper where a series of six articles in August 1835 told how astronomer John Herschel, using a great telescope of new (and in fact impossible) design in South Africa, had observed amazing geological formations and a great variety of life-forms on (and flying above) the surface of the Moon...

Of course, this message is off-topic. Questions such as how to determine which information source to trust have no Risks relevance whatever. :-)

Mark Brader "Never trust anybody who says 'trust me.'
Toronto Except just this once, of course." John Varley,
"Steel Beach"



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 89

Monday 29 May 2000

Contents

- [Top-secret stolen UK laptop recovered](#)
[Doneel Edelson](#)
- [Nuclear reactor shuts down in California](#)
[Linda Kaplan](#)
- [Venezuela cites computer glitch, postpones elections](#)
[Declan McCullagh](#)
- [NHL Web attack](#)
[Keith A Rhodes](#)
- [A rather risky device to end high-speed chases](#)
[Serguei Patchkovskii](#)
- [Media gullibility on laser gun to stop cars](#)
[John Pettitt](#)
- [Study shows mobile phones do interfere with avionics](#)
[Kevin Connolly](#)
- [Junk-mail filters: excerpted](#)
[Gary Cattarin](#)
- [Revision control](#)
[Mike Albaugh](#)
- [Outlook "security" patch](#)
[Dave Weingart](#)

- [VBS.NewLove.A false positives](#)
[Jeremy Epstein](#)
 - [Risks of virus disinfection](#)
[Tom Hayhurst](#)
 - [Widespread Web-Trojan alerts](#)
[Chris Adams](#)
 - [CERT Advisory CA-2000-07](#)
[CERT](#)
 - [Misleading warning, failure of Netscape SSL server authentication](#)
[Kevin Fu](#)
 - [I did not say that! wrt deja.com](#)
[Stephen Keeling](#)
 - [Risky quotation](#)
[Zygo Blaxell](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Top-secret stolen UK laptop recovered**

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

Mon, 22 May 2000 16:32:55 -0400

A stolen laptop computer holding details of a top secret 250-billion-pound Anglo-US super-lethal stealth Strike fighter project has been recovered by *The Mirror*. The laptop was stolen from a naval intelligence officer at a London station two weeks before. [Source: *Mirror* article 22 May 2000 <<http://www.sundaymirror.co.uk>> <<http://www.people.co.uk>>; PGN-ed]

⚡ **Nuclear reactor shuts down in California**

Queen of infinite Space)" <Linda.Kaplan@eng.sun.com ("Rainbow">
15 May 2000 11:21:49 -0700

Due to an electrical problem at 12:25 a.m. on 15 May 2000, an automated shutdown of a Diablo Canyon Unit 1 nuclear power plant reactor released a small amount of radioactive steam. Everything seemed to function properly in the triggered shutdown. [Source: An AP item on 15 May 2000]

🔥 Venezuela cites computer glitch, postpones elections

Declan McCullagh <declan@well.com>
Fri, 26 May 2000 11:30:11 -0400

CARACAS, VENEZUELA -- Citing technical woes, Venezuela's high court on Thursday suspended this weekend's general elections, saying fair balloting is impossible until the problems are resolved. Conditions for "credibility and transparency" in Sunday's presidential, congressional and regional elections do not exist, said Ivan Rincon of the Supreme Tribunal of Justice. [...] President Hugo Chavez had earlier blamed an Omaha (Neb.)-based company for the technical problems, saying it was part of an overall plan to "destabilize" the country's electoral process. [Source: Citing major computer woes, high court delays elections *Chicago Tribune*, 26 May 2000

<http://www.chicagotribune.com/news/printedition/article/0,2669,SAV-0005260364,FF.html>;

PGN-ed; see also:

<http://www.washingtonpost.com/wp-dyn/articles/A7231-2000May25.html>

http://www.foxnews.com/world/0523/i_ap_0523_111.sml
http://news.bbc.co.uk/low/english/world/americas/newsid_764000/764372.stm

[Contrast the controversy over the recent election in Peru.
PGN]

⚡ NHL Web attack

"Keith A Rhodes" <rhodesk.aimd@gao.gov>
Fri, 26 May 2000 07:53:22 -0400

Add the National Hockey League to the long list of sites that have been attacked. A distributed denial of service attack on the NHL Web site took it off the air for several days, 21 through 25 May. The rather long period was blamed by the NHL's Web manager on their lack of technical resources, and chalked it up as a learning experience. [Source: NHL Web Site Back Online, Associated Press item, 26 May 2000]

⚡ A rather risky device to end high-speed chases

"Serguei Patchkovskii" <patchkov@ucalgary.ca>
Sun, 14 May 2000 9:54:14 MDT

High-speed police chases have been a rather hot topic in Canadian media recently. Larry Martens, a 22-year veteran former Mountie (RCMP), has a patent on a radio device that would allow police to stop the engine of any fleeing vehicle at the push of a button. Every vehicle would require a \$150

receiver. [Source: Device could end high-speed chases, by Scott Crowson, *Calgary Herald*, city section, 14 May 2000; PGN-ed]

Sounds like a worthwhile addition to "1000 ways of having fun with a police scanner" to me. [SP]

home page: <http://www.cobalt.chem.ucalgary.ca/ps/>

✶ Media gullibility on laser gun to stop cars

John Pettitt <jpp@cloudview.com>

Thu, 18 May 2000 23:11:25 -0700

After a recent car chase that ended with the fugitive jumping off the Golden Gate Bridge there was an item on the TV (NBC national news) about a new device being promoted to enable police to stop any car using a "laser gun". This caught my attention, mostly because it didn't sound reasonable. Indeed the secret was revealed at the end of the story when the reporter said that for the device to work all cars would need to be fitted with an "inexpensive receiver".

There is so much wrong with this idea it's hard to know where to start; even if the system was designed well enough that only "real" guns would work (very unlikely IMHO) a stolen "gun" could create total gridlock in a city.

Perhaps the biggest risk here is that NBC actually ran the item without stopping to notice how silly the idea was.

John

✶ Study shows mobile phones do interfere with avionics

Kevin Connolly <Kevin.Connolly@ck.cit.alcatel.fr>

Mon, 29 May 2000 09:14:13 +0100

See <http://www.newscientist.com/nsplus/insight/phones/dangersignals.html>

The study showed that mobiles caused problems for older generation avionics during tests in a parked jet.

"interference levels that exceed demonstrated susceptibility levels for aircraft equipment approved against earlier standards"

Kevin Connolly

✶ Junk-mail filters

"Gary Cattarin" <gcattari@nortelnetworks.com>

Fri, 19 May 2000 11:41:41 -0700

[NOTE: Entire item in [RISKS-20.89x](#). See below. PGN]

This I'm sure has been covered before, but here's an interesting example of filters gone awry.

I recently upgraded (?) to MS Office 2000, which, among other things, lets you have more than 8 e-mail filters active at once. In my glee I started

turning things on, including junk mail filtering. Surprise! I found 8-10 important messages -- all replies to a query I sent out to a personal mailing list -- all dumped into the Junk Mail folder.

What was it? I'm riding in a charity bicycle ride, and I needed to tell my pledge-ees that I needed their money now. So I sent them an e-mail updating my training status and asking them to send their checks. Obviously, this message had at least one dollar sign "\$" in it -- and because I'm an excitable guy it had at least one multiple exclamation mark "!!", and since, at the end, I chided my manager to make good on my exaggerated version of his pledge:

>> Mark, didn't you promise \$5,000 or something like that?

...we also hit the magic phrase ",000".

Now, the fine folks in Redmond have determined that if these three elements converge, you have received Spam. The actual rule (from their web site) is:

Body contains ",000" AND Body contains "!!" AND Body contains "\$"

Who'd have guessed? In fact, even looking at their filter list, it took me a long time to figure out which rule I'd hit. (OK, I'm slow sometimes.)

I guess the rule is (a) don't get too excited ! -- one "!" at a time! (b) specify your currency as "USD", and (c) use European periods ("5.000") instead of North American commas in large numbers. OK, that's silly. But

just as silly is the fact that any spammer can read the list of rules and tailor their e-mail to avoid them.

Of course, you might never read this, because if you have junk e-mail filtering turned on, Outlook will catch THIS message and do with it as you've requested for junk mail.

Two other interesting points:

(1) In the adult filters you'll find these two:

Subject contains " sex"

Subject contains "free" AND Subject contains "sex"

The first is set up with a leading space to only accept the *word* "sex", so

those of us who live here in Middlesex county don't lose any local-related

mail. But the writer of the second wasn't so careful -- what if the

Middlesex News offers free subscriptions? That's Spam, yes, but not porn (I

guess that's why that newspaper changed its name...).

(2) Don't address your dear friend as such -- note the rule:

Body contains "Dear friend"

My golly! I can't send some good old-fashioned heartfelt feelings to my

dear friends!! (oops, double "!!" -- I got excited!)

This stuff can be very dangerous...

The entire list is at

<http://officeupdate.microsoft.com/Articles/newfilters.htm>

I included it here, but the moderator may choose to cut it from the journal

in the interest of space.

[Your moderator chose to create a supplemental issue,

[RISKS-20.89x](#)

that contains the complete original submission. I would have included it here, but it is likely to have greatly increased

the

likelihood that the entire RISKS issue would be bounced by many filtering programs. As it is, I frequently get porn-bounce or spam-bounce notices on seemingly harmless issues of RISKS. PGN]

✂ Revision control

Mike Albaugh <albaugh@agames.com>

Thu, 25 May 2000 11:03:35 -0700 (PDT)

When I heard that Microsoft was considering action against the person[s] responsible for the "Weenie" security hole, "_If they can be found_", my first thought was along the lines of "These guys don't even have revision-control on _security_ software?!?", but yesterday morning my clock-radio woke me up to even more startling news. In a story about the egregious expansion of search-and-seizure that was added to the new "Bankruptcy Reform" bill, was the news that the Senate apparently did not _know_ who had inserted the language, but believed it was the work of a staffer in Orin Hatch's office. Now, maybe I was still too groggy, but my reaction to this was "These guys don't even have revision-control on _laws_?!?". I wish I could add a :-), but the consequences are potentially far worse than one more bug in software well known for security weaknesses. The fact that the suspect language was apparently "included by reference" from an un-related bill is yet another example of the hazards of abstraction. IMHO, we as a society place entirely too much trust in

un-trustworthy components and agents.

Note also the parallels to the debate on Open Source. _In Principle_, every congressperson would read (and understand) every word of every bill (and follow/verify references). In practice, only by chance do these alterations become known.

Mike albaugh@agames.com

⚡ Outlook "security" patch

Dave Weingart <dave.weingart@us.randstad.com>

Thu, 18 May 2000 11:15:50 -0400

Microsoft has decided that since the scripting behavior of Outlook is unsafe, they're going to disable the ability to actually get many file attachments (it's not entirely clear if the file will be saved or simply trashed -- it seems to imply that you can't access the attachments within Outlook 98 and Outlook 2000 only. If the file is completely trashed, a whole new RISK is created by people assuming that an e-mailed attachment got through).

<http://www.officeupdate.com/2000/articles/Out2ksecarticle.htm> has Microsoft's official word on the update.

Dave Weingart, Randstad North America dave.weingart@us.randstad.com
1-516-682-1470

⚡ VBS.NewLove.A false positives

"Jeremy Epstein" <jepstein@webmethods.com>

Fri, 19 May 2000 17:58:53 -0400

As everyone knows, VBS.NewLove.A is sweeping the world. Or is it? Norton AntiVirus, using the latest set of definition files (5/18/00) is giving false positives on a range of files. On my system, it's complaining about some pure HTML files (i.e., with no scripting or anything else remotely malicious). Their web page doesn't give any details, and I haven't been able to find anything out, but their technicians did admit to false positives, and they're working on a new version.

In fairness to Symantec, they're trying to rush out patches as fast as they can to a rapidly proliferating virus. However, it's obvious that they didn't do a very good job of getting the pattern match correct.

--Jeremy

⚡ Risks of virus disinfection

"Tom Hayhurst" <aserinsky@hotmail.com>

Thu, 25 May 2000 15:51:33 GMT

In the aftermath of the Love Bug, all e-mail inboxes at my place of employment have been scanned for suspect attachments. Apparently, a home-grown perl script (run as root) was used to delete or

modify tainted e-mails. Unfortunately, a side-effect of this was to make all files in the mail spool directory world-readable about ten days ago. This has only just been noticed and rectified.

Obvious Risk: immediate, disruptive threats can divert attention away from safe, well-known procedures.

Tom Hayhurst <aserinsky@hotmail.com>

🔥 Widespread Web-Trojan alerts

Chris Adams <chris@improbable.org>

Mon, 15 May 2000 08:17:29 -0700

The people at Zope found a problem with their admin interface (<http://www.zope.org/Members/jim/ZopeSecurity/ClientSideTrojan>) that also applied to just about any web-based admin tool. Basically, an attacker could create a page that redirected to site's admin interface or a form that submitted to it (possibly using JavaScript for automatic submission); in any case, the effect was that any user who was logged in as a site administrator could have an attacker execute arbitrary commands in their security context merely by following a link. If this was carefully set up using JavaScript and frames, it's more than possible that the admin would never notice what had happened. This attack would be particularly effective against online news sites and anyone else for whom it is common to receive many URLs every

day as submissions.

This story was picked up by LWN (<http://www.lwn.net/2000/features/Redirect.phtml>) and spread rapidly to the usual security forums.

There's a very simple fix that prevents this attack from working in any of the cases reported. The problem is that the form parameters can all be guessed by the attacker, allowing them to generate a URL easily. Putting in a random parameter prevents this from being true. Given that you need to have a random identifier that is not leaked to third parties for meaningful session management, an obvious step is to put in a parameter in the form that must match the user's session ID (e.g. Confirm=346593045 instead of Confirm=true).

(This is still vulnerable if the browser has a security hole which allows an unrelated site to capture cookies. However, such a bug is really a separate issue as it would allow an attacker to easily hijack the session directly. A browser that buggy should not be used.)

What I've found disturbing is that there have been several people attempting to get the news out since the original wave of reports (~5/10) about having such a fix that will defang this entire class of attack in a single line of code. These efforts don't seem to have achieved anything like the visibility given to the original reports. There's a great deal of speculation about convoluted, partial means of stopping such attacks and even suggestions about disabling web-based admin interfaces entirely but, thus

far, very
little word about what has to be one of the easiest fixes in the
history of
computer security.

The risks? Besides the obvious security concerns, there's the
risk that
people will do something rash or remain vulnerable despite the
fact that,
contrary to some of the reports, there is a fix and it's quite
simple. A
casual observer could easily get the impression that this
problem is a major
threat.

🔥 CERT Advisory CA-2000-07 [Abridged for RISKS]

CERT Advisory <cert-advisory@cert.org>

Wed, 24 May 2000 15:54:49 -0400 (EDT)

CERT Advisory CA-2000-07 Microsoft Office 2000 UA ActiveX Control
Incorrectly Marked "Safe for Scripting"

[The full Advisory is at

<http://www.cert.org/advisories/CA-2000-07.html>

PGN]

Systems Affected

- * Systems with Internet Explorer and Microsoft Office 2000
components, including
 - * Word 2000
 - * Excel 2000
 - * PowerPoint 2000
 - * Access 2000
 - * Photodraw 2000
 - * FrontPage 2000
 - * Project 2000

- * Outlook 2000
- * Publisher 2000
- * Works 2000 Suite

Overview

The Microsoft Office 2000 UA ActiveX control is incorrectly marked as "safe for scripting". This vulnerability may allow an intruder to disable macro warnings in Office products and, subsequently, execute arbitrary code. This vulnerability may be exploited by viewing an HTML document via a web page, newsgroup posting, or e-mail message.

I. Description

Microsoft and L0pht Research Labs have recently published advisories describing a vulnerability in the Microsoft Office 2000 UA ActiveX control. Due to the severity of this vulnerability, we are issuing a CERT advisory to help reach as broad an audience as possible.

Microsoft has published a security bulletin, an FAQ, and a knowledgebase article describing this vulnerability. These documents are available from Microsoft's web site:

<http://microsoft.com/technet/security/bulletin/ms00-034.asp>
<http://microsoft.com/technet/security/bulletin/fq00-034.asp>
<http://microsoft.com/technet/support/kb.asp?ID=262767>

The CERT Coordination Center thanks L0pht Research Labs and @Stake for initially discovering and reporting this vulnerability. We also thank the Microsoft Security Team for their assistance in preparing this advisory.

⚡ Misleading warning, failure of Netscape SSL server authentication

Kevin Fu <fubob@MIT.EDU>

Fri, 26 May 2000 09:51:05 EDT

Here is an example where improper caching and poor GUI design can render a particular implementation of SSL server authentication insecure.

Within one Netscape session, if a user clicks on "continue" in response to a "hostname does not match name in certificate," then that certificate is incorrectly validated for future use in the Netscape session, REGARDLESS of the hostname or IP address of other servers that use the certificate.

It seems that the "Certificate Name Check" warning will cache a certificate as valid for any hostname or IP address in the future. In this way, if an adversary tricks a user into accepting an invalid certificate at a seemingly benign site, then the user can then be tricked if he/she ever visits a malicious site using the same certificate. A "continue" click on a seemingly benign SSL web server might end up taking away server authentication from visiting <https://www.a-site-that-you-give-private-info.com/> that has poisoned DNS.

Since this is a risks post, there has to be a lesson:

- * Be explicit. Netscape's security warning does not indicate clearly what will result by clicking "continue."

* Even if the design is good, an implementation can go wrong. Netscape invented SSL, but it has a hard time using it correctly.

Does this scare you? It should. If a company who designs an accepted security protocol cannot use it correctly, then think about the companies implementing homebrew security...

* Implementation bugs are not unique to Netscape. PGP has a relatively good but absolutely dangerous user interface that can

mislead users. See the "Why Johnny Can't Encrypt" paper by Alma

Whitten for an excellent analysis. [SEE NOTE]

For a full report, see

<http://snafu.fooworld.org/~fubob/netscape-ssl.html> or

<http://www.cert.org/advisories/CA-2000-08.html>

Kevin E. Fu (fubob@mit.edu)

[NOTE: The paper must be Whitten in Inwisible Ink. PGN-Enquipped]

⚡ I did not say that! wrt deja.com

"s. keeling" <keeling@spots.ab.ca>

Wed, 24 May 2000 01:01:12 -0600

I don't know if this is a problem or if I'm over reacting. I just did a search on my user id and chanced across a misquoted (by some usenet newbie) news article that attributes statements I never said to me.

[http://x69.deja.com/\[ST_rn=fs\]/getdoc.xp?](http://x69.deja.com/[ST_rn=fs]/getdoc.xp?)

[AN=624428330&CONTEXT=959150860.1906835472&hitnum=6](http://x69.deja.com/[ST_rn=fs]/getdoc.xp?AN=624428330&CONTEXT=959150860.1906835472&hitnum=6)

Do people take deja/usenet with a grain of salt, or should I

worry
about what anyone can say I said?

keelingNO@SPAM.spots.ab.ca (Stephen) TopQuark Software & Serv.

[Misinformation has a horrible way of propagating. If I were you, I would

put a note on your Web site disowning something like that and perhaps

putting in a thoughtful item on the risks of being misquoted.
PGN]

⚡ Risky quotation

Zygo Blaxell <uryse0d5@umail.furryterror.org>
22 May 2000 23:25:38 -0400

While at a bookstore the other day, my spouse was presented with a credit card signature slip printed by an Interac point-of-sale terminal. It was just like any other credit signature slip, except that the usual "customer signature" line was printed twice, one on top of the other, with ample space for the signature in both places--a harmless glitch, probably due to an obvious and simple programming error.

We pointed the error out to the cashier, who was probably barely old enough to be legally employed, and her response, if she speaks for her generation, was ominous, even terrifying:

"It does that because ... because it's a computer."

An entire generation is growing up believing that the current sorry state of affairs in information technology could ever be accepted as

normal!



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 90

Monday 5 June 2000

Contents

- ["Incompatible software" blamed for phone-book fiasco](#)
[PGN](#)
- [Remote control of your car via GM's OnStar](#)
[Armando Fox](#)
- [India plans to piggyback internet on railway control cables](#)
[R Bakowski](#)
- [Trash compactor kills shoplifter](#)
[Chris Meadows](#)
- [How not to distribute white papers](#)
[Avi Rubin](#)
- [1984 comes late to the UK](#)
[Martyn Thomas](#)
- [Social engineering in the real world](#)
[Bruce Schneier](#)
- [Computer Security: Will We Ever Learn?](#)
[Bruce Schneier](#)
- [Symantec's antiviral returns false positives on network.vbs](#)
[Richard Thieme](#)
- [Re: Junk-mail filters](#)
[Amos Shapir](#)

[Ron Bean](#)

[Ray Todd Stevens](#)

[Markus Peuhkuri](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ "Incompatible software" blamed for phone-book fiasco

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

Mon, 5 Jun 2000 11:39:08 PDT

Pacific Bell has apparently printed 400,000 new phone books that include names, phone numbers, and addresses of telephone customers who are supposed to be unlisted. The California state public utilities commission has granted a request from Cox Communications for a restraining order against Pac*Bell. Incompatible software is blamed, but perhaps it was human error in forgetting to remove the protected fields from a retrieval request? Perhaps one of our RISKS-reading insiders can enlighten us.

⚡ Remote control of your car via GM's OnStar

"Armando Fox" <fox@cs.stanford.edu>

Wed, 31 May 2000 15:33:20 -0700

At WWW-9 in May, there was a presentation about the OnStar system which will be standard equipment on some GM vehicles and a factory-installed option on most others. OnStar uses cellular telephony and GPS to provide location-specific services to drivers; current services are provided by a

human being ("advisor") who answers the phone when you push the OnStar button in your car, but there is provision for data services to be delivered later. Look at <http://www.onstar.com> - the system is already in production operation in some cars.

One interesting feature is a control channel back *into* the car: the OnStar transceiver is integrated with some of your car's control systems, so that it can (upon receipt of the correct signal from an OnStar advisor) unlock the doors, flash the headlights, honk the horn, etc. Presumably some of these features are in place to assist rescue personnel -- OnStar automatically dials a 911 advisor if it detects you've had an accident (e.g. if it detects that the airbag was deployed).

The obvious risk: If I were a cell phone data services hacker, I'd know what my next project would be. I asked the OnStar speaker what security mechanisms were in place to prevent your car being hacked. He assured me that the mechanisms in place were "very secure". I asked whether he could describe them, but he could not because they were also "very proprietary".
Sigh

Armando Fox <fox@cs.stanford.edu>, Assistant Professor, Computer Science
Stanford, CA 94305-9040 +1 650 723 9558 <http://gunpowder.stanford.edu/~fox>

🔥 India plans to piggyback internet on railway control cables

"R Bakowski" <ron@belwood.com>

Wed, 31 May 2000 08:05:58 -0400

May 30, 2000

http://news.bbc.co.uk/hi/english/world/south_asia/newsid_769000/769635.stm

As reported by the BBC today, India has embarked on a pilot project to bring affordable Internet service to rural India by exploiting the "almost always" available spare capacity of the electrified railway tracks' communications and control cabling. Included in the plan are cybercafe kiosks at railway stations along the project's initial 40km stretch of track as well as wireless service from one of the stations to surrounding homes. There are more than 60,000 km of railway in India.

Looks like an accident waiting for a moment to happen.

Ron Bakowski, Belwood Information Technologies Inc. ron@belwood.com

✶ Trash compactor kills shoplifter

Robotech_Master <robotech@eyrie.org>

Wed, 31 May 2000 22:53:46 -0500

Not a risk of a computer per se, but a risk of automation.

In the tradition of the reluctant mobster's "pressing engagement" in Goldfinger, it seems a hapless shoplifter, looking for a place to hide, dived into a trash compactor...which triggered automatically,

crushing her
to death.

The whole story is at

<URL:<http://www.cnn.com/2000/US/05/31/compactor.death.ap/index.html>> but

particularly noteworthy is the line, "The compactor starts automatically when it senses a certain weight, [Police Officer Glen Woods] said." The risk inherent in such a weight-related trigger should be readily apparent.

Chris Meadows aka Robotech_Master <URL:<http://www.eyrie.org/~robotech/>>

robotech@eyrie.org robotech@jurai.net ICQ UIN: 5477383

⚡ How not to distribute white papers

Avi Rubin <rubin@research.att.com>

Thu, 1 Jun 2000 17:45:34 GMT

I was reading a white paper from Microsoft about Windows 2000 security.

In particular, I am interested in how the Encrypted File System (EFS)

works. Someone at Microsoft informed me that there was a new version of

the white paper available at

<http://www.microsoft.com/windows2000/library/howitworks/security/encrypt.asp>

Great. I went to that site, and I found a copy of the introduction and a

link to the paper. The only catch was that the only way to download the

paper is to download a file called encrypt.exe. Once you download this file,

you can run the program, which unzips a word file. Obviously,

Microsoft is doing this to save storage space on their server and to reduce latency on the downloads.

Of all companies, Microsoft should be the last one to encourage users to get into the habit of downloading .exe programs and running them. The way I handled it was to download the file to a sacrificial machine that I use for this purpose. Then, I took it off the network and ran the program. I then physically copied the .doc file to a floppy and transferred it using sneakernet to my regular PC. Of course, I was still taking a chance. If the downloaded program were malicious, then it could do its damage the next time I connect the machine to the network. The problem is that it is very difficult to know that a program is harmless, just because it does something that you expect it to do. I could not believe that this is how Microsoft distributes its white papers. It is beyond comprehension.

Avi Rubin

<http://avirubin.com/>

1984 comes late to the UK

"Martyn Thomas" <mct@hollylaw.demon.co.uk>

Mon, 29 May 2000 23:10:35 +0100

The Regulation of Investigatory Powers Bill has just been passed by the UK House of Commons.

Amongst other provisions, the Bill contains powers to force all ISPs to introduce mechanisms to copy all internet traffic to a Government interception agency in real time. Whilst the data should only be disclosed to a limited set of agencies following senior authorisation (itself a profound erosion of civil liberty) the "traffic data" (defined to include the URLs of pages accessed) is available to any public authority for almost any purpose it considers part of its normal business.

Encryption? The Bill gives the police and security services the power to demand keys. You've lost them? Prove it [how?] or go to jail for 2 years.

Want to complain? You can be served with a gagging order that requires that you tell no-one that your keys (or their keys) have been compromised, on penalty of five years in jail.

The Bill starts in the House of Lords in two weeks time, but seems likely to pass without substantial weakening.

The risk? Why would any business (or anyone else) want to use any UK-based ISP under these circumstances?

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

Social engineering in the real world

Bruce Schneier <schneier@counterpane.com>
Tue, 30 May 2000 22:14:02 -0500

<http://www.cnn.com/2000/US/05/25/security.breaches.01/index.html>

The best line is:

"I think any time you expose vulnerabilities it's a good thing,"
said

Attorney General Janet Reno....

This, of course, means that she is in favor of full disclosure
of network
vulnerabilities.

Bruce Schneier, CTO, Counterpane Internet Security, Inc. Ph:
408-556-2401

3031 Tisch Way, 100 Plaza East, San Jose, CA 95128 Fax:
408-556-0889

✶ Computer Security: Will We Ever Learn? (CRYPTO-GRAM, May 15, 2000)

Bruce Schneier <schneier@counterpane.com>

Mon, 15 May 2000 15:06:31 -0500

[From CRYPTO-GRAM, May 15, 2000, in RISKS with permission, by
Bruce

Schneier, Counterpane Internet Security, Inc.
<schneier@counterpane.com>

See Bruce's free Internet security newsletter: <http://www.counterpane.com>]

Computer Security: Will We Ever Learn?

If we've learned anything from the past couple of years, it's
that computer
security flaws are inevitable. Systems break, vulnerabilities
are reported
in the press, and still many people put their faith in the next
product, or

the next upgrade, or the next patch. "This time it's secure," they say. So far, it hasn't been.

Security is a process, not a product. Products provide some protection, but the only way to effectively do business in an insecure world is to put processes in place that recognize the inherent insecurity in the products. The trick is to reduce your risk of exposure regardless of the products or patches.

Consider denial-of-service attacks. DoS attacks are some of the oldest and easiest attacks in the book. Even so, in February 2000, coordinated, distributed DoS attacks easily brought down several high-traffic Web sites, including Yahoo, eBay, Amazon.com and CNN.

Consider buffer overflow attacks. They were first talked about as early as the 1960s -- time-sharing systems suffered from the problem -- and were known by the security literati even earlier than that. In the 1970s, they were often used as a point of attack against early networked computers. In 1988, the Morris Worm exploited a buffer overflow in the Unix fingerd daemon: a very public use of this type of attack.

Today, over a decade after Morris and about 35 years after these attacks were first discovered, you'd think the security community would have solved the problem of security vulnerabilities based on buffer overflows. Think again. Over two-thirds of all CERT advisories in 1998 were for vulnerabilities caused by buffer overflows. During an average week in 1999, buffer overflow vulnerabilities were found in the RSAREF

cryptographic toolkit (oops), HP's operating system, the Solaris operating system, Microsoft IIS 4.0 and Site Server 3.0, Windows NT, and Internet Explorer. A recent study named buffer overflows as the most common security problem.

Consider encryption algorithms. Proprietary secret algorithms are regularly published and broken. Again and again, the marketplace learns that proprietary secret algorithms are a bad idea. But companies and industries -- like Microsoft, the DVD consortium, cellular phone providers, and so on -- continue to choose proprietary algorithms over public, free alternatives.

Is Anyone Paying Attention?

Sadly, the answer to this question is: not really. Or at least, there are far fewer people paying attention than should be. And the enormous need for digital security products necessitates people to design, develop and implement them. The resultant dearth of experts means that the percentage of people paying attention will get even smaller.

Most products that use security are not designed by anyone with security expertise. Even security products are generally designed and implemented by people who have only limited security expertise. Security cannot be functionality tested -- no amount of beta testing will uncover security flaws -- so the flaws end up in fielded products.

I'm constantly amazed by the kinds of things that break security

products. I've seen a file encryption product with a user interface that accidentally saves the key in the clear. I've seen VPNs where the telephone configuration file accidentally allows a random person to authenticate himself to the server, or that allows one remote client to view the files of another remote client. There are a zillion ways to make a product insecure, and manufacturers manage to stumble on a lot of those ways again and again.

No one is paying attention because no one has to.

Computer security products, like software in general, have a very odd product quality model. It's unlike an automobile, a skyscraper, or a box of fried chicken. If you buy a product, and get harmed because of a manufacturer's defect, you can sue...and you'll win. Car-makers can't get away with building cars that explode on impact; chicken shops can't get away with selling buckets of fried chicken with the odd rat mixed in. It just wouldn't do for building contractors to say thing like, "Whoops. There goes another one. Sorry. But just wait for Skyscraper 1.1; it'll be 100% collapse-free!"

Software is different. It is sold without any claims whatsoever. Your accounts receivable database can crash, taking your company down with it, and you have no claim against the software company. Your word processor can accidentally corrupt your files and you have no recourse. Your firewall can turn out to be completely ineffectual -- hardly better than

having nothing at all -- and yet it's your fault. Microsoft fielded Hotmail with a bug that allowed anyone to read the accounts of 40 or so million subscribers, password or no password, and never bothered to apologize.

Software manufacturers don't have to produce a quality product because there is no liability if they don't. And the effect of this for security products is that manufacturers don't have to produce products that are actually secure, because no one can sue them if they make a bunch of false claims of security.

The upshot of this is that the marketplace does not reward real security. Real security is harder, slower, and more expensive, both to design and to implement. Since the buying public has no way to differentiate real security from bad security, the way to win in this marketplace is to design software that is as insecure as you can possibly get away with.

Microsoft knows that reliable software is not cost effective. According to studies, 90% to 95% of all bugs are harmless. They're never discovered by users, and they don't affect performance. It's much cheaper to release buggy software and fix the 5% to 10% of bugs people find and complain about.

Microsoft also knows that real security is not cost-effective. They get whacked with a new security vulnerability several times a week. They fix the ones they can, write misleading press releases about the ones they can't, and wait for the press fervor to die down (which it always

does). And six months later they issue the next software version with new features and all sorts of new insecurities, because users prefer cool features to security.

The only solution is to look for security processes.

There's no such thing as perfect security. Interestingly enough, that's not necessarily a problem. In the U.S. alone, the credit card industry loses \$10 billion to fraud per year; neither Visa nor MasterCard is showing any sign of going out of business. Shoplifting estimates in the U.S. are currently between \$9.5 billion and \$11 billion per year, but you never see "shrinkage" (as it is called) cited as the cause when a store goes out of business. Recently, I needed to notarize a document. That is about the stupidest security protocol I've ever seen. Still, it works fine for what it is.

Security does not have to be perfect, but the risks have to be manageable. The credit card industry understands this. They know how to estimate the losses due to fraud. Their problem is that losses from phone credit card transactions are about five times the losses from face-to-face transactions (when the card is present). Losses from Internet transactions are many times those of phone transactions, and are the driving force behind SET.

My primary fear about cyberspace is that people don't understand the risks, and they are putting too much faith in technology's ability to obviate

them. Products alone cannot solve security problems.

The digital security industry is in desperate need of a perceptual shift. Countermeasures are sold as ways to counter threats. Good encryption is sold as a way to prevent eavesdropping. A good firewall is a way to prevent network attacks. PKI is sold as trust management, so you can avoid mistakenly trusting people you really don't. And so on.

This type of thinking is completely backward. Security is old, older than computers. And the old-guard security industry thinks of countermeasures not as ways to counter threats, but as ways to avoid risk. This distinction is enormous. Avoiding threats is black and white: either you avoid the threat, or you don't. Avoiding risk is continuous: there is some amount of risk you can accept, and some amount you can't.

Security processes are how you avoid risk. Just as businesses use the processes of double-entry bookkeeping, internal audits, and external audits to secure their financials, businesses need to use a series of security processes to protect their networks.

Security processes are not a replacement for products; they're a way of using security products effectively. They can help mitigate the risks. Network security products will have flaws; processes are necessary to catch attackers exploiting those flaws, and to fix the flaws once they become public. Insider attacks will occur; processes are necessary to detect the attacks, repair the damages, and prosecute the attackers. Large

systemwide flaws will compromise entire products and services (think digital cell phones, Microsoft Windows NT password protocols, or DVD); processes are necessary to recover from the compromise and stay in business.

Here are two examples of how to focus on process in enterprise network security:

1. Watch for known vulnerabilities. Most successful network-security attacks target known vulnerabilities for which patches already exist. Why? Because network administrators either didn't install the patches, or because users reinstalled the vulnerable systems. It's easy to be smart about the former, but just as important to be vigilant about the latter. There are many ways to check for known vulnerabilities. Network vulnerability scanners like Netect and SATAN test for them. Phone scanners like PhoneSweep check for rogue modems inside your corporation. Other scanners look for Web site vulnerabilities. Use these sorts of products regularly, and pay attention to the results.
2. Continuously monitor your network products. Almost everything on your network produces a continuous stream of audit information: firewalls, intrusion detection systems, routers, servers, printers, etc. Most of it is irrelevant, but some of it contains footprints from successful attacks. Watching it all is vital for security, because an attack that bypassed one product might be picked up by another. For example, an attacker might exploit a flaw in a firewall and bypass an IDS, but his

attempts to get root access on an internal server will appear in that server's audit logs. If you have a process in place to watch those logs, you'll catch the intrusion in progress.

In this newsletter and elsewhere I have written pessimistically about the future of computer security. The future of computers is complexity, and complexity is anathema to security. The only reasonable thing to do is to reduce your risk as much as possible. We can't avoid threats, but we can reduce risk.

Nowhere else in society do we put so much faith in technology. No one has ever said, "This door lock is so effective that we don't need police protection, or breaking-and-entering laws." Products work to a certain extent, but you need processes in place to leverage their effectiveness.

Copyright (c) 2000 by Counterpane Internet Security, Inc.
Bruce Schneier, CTO, Counterpane Internet Security, Inc. Ph:
408-556-2401
3031 Tisch Way, 100 Plaza East, San Jose, CA 95128 Fax:
408-556-0889

[A version of this essay originally appeared in the April issue of

Information Security magazine.

<<http://www.infosecuritymag.com/apr2000/cryptorhythms.htm>>]

🔥 Symantec's antiviral returns false positives on network.vbs

Richard Thieme <rthieme@thiemeworks.com>

Tue, 30 May 2000 11:44:34 -0500

And that's just the beginning.

When the alert from Symantec's Systemworks 2000 Anti Virus told me an e-mail carried the network.vbs worm, I followed steps to quarantine the file. By the time the alert sounded again - on another email - I realized that it was detecting not the worm itself but the source code for the worm which was included in e-mails on a security list to which I subscribe. The first alert had isolated the entire e-mail box on Eudora Pro to which a filter directed that e-mail. The second time, it would have done the same to my inbox, with all of the stored e-mail in it. I copied the e-mail out of my inbox, deleted and recreated an inbox, then rebooted and transferred the e-mail back to the inbox. But that other mailbox was in quarantine. I struggled in vain to reach someone at Symantec - they want \$30 up front to tell them that they made a mistake - so I tried their web site response forms. That of course brought me nothing but a rash of documents sent by automated processes about all the recent .vbs worms but of course not one answered my question, i.e., how can I get my e-mail box out of quarantine? So I sent the quarantined "file" to Symantec with a note asking for the contents of the e-mail box back. No human being read that note either - I received an automated reply telling me that the file was a clean text file with no virus (duh), and when I finally was able to contact a human being after more hours of voice mail and round-about calls, I reached a "help technician" who had no idea what to

do ("the guy who knows these things isn't here today") so he asked around until he could tell me that the file was destroyed - like that village in Viet Nam - in order to save it. I asked what one had to do to get the contents of a quarantined file back and he said no one ever requested that before.

Procedural errors, inadequate training, human mistakes, automated replies that are irrelevant, voice mail hell, screw-the-customer costs, it's-your-problem-not-ours -- it's all here in this scenario, my e-mail file is gone, and now when I am now told by Symantec Anti Virus that e-mail has arrived with network.vbs on it, I know that I should -- do what, exactly?

Richard Thieme, ThiemeWorks, PO Box 170737, Milwaukee Wisconsin 53217-8061
1-414.351.2321 cell: 1-414.704.4598 <http://www.thiemeworks.com>

✶ Re: Junk-mail filters (Cattarin, [RISKS-20.89](#))

<amos@nsof.co.il>

Wed, 31 May 2000 18:16:31 IDT

> Body contains [...]

Ooops!

> [Your moderator chose to create a supplemental issue,
> [RISKS-20.89x](#)

Too late... The first line I quoted above was probably the reason why this issue of RISKS was not posted on the news server I use (and

of
course neither was the [20.89x](#) issue), so I had to pull them
directly off
your site by FTP. I hope this message goes through!

Amos Shapir, nSOF Parallel Software, Ltd., Givat-Hashlosha
48800, Israel
Tel: +972 3 9388551 Fax: +972 3 9388552

[Also noted by Timothy Prodin.

NOTE TO READERS: If you did not receive [RISKS-20.89](#), it was
undoubtedly the victim of filtering. Try the archives. PGN]

✉ Re: Junk-mail filters (Cattarin, [RISKS-20.89](#))

"Ron Bean" <rbean@execpc.com>

Thu, 1 Jun 2000 10:09:18 -0500 (CDT)

A couple of years ago I put together a procmail filter using
similar kinds
of rules. However, the first rule I used was to delete any Bcc:
mail that
comes from an unknown source (ie, a From: address that's not on
a list of
friends, relatives, business contacts, subscribed mailing lists,
etc). My
log files showed that 96% of the spam was being deleted by the
Bcc: filter
and not even getting to the "clever" ones. So I just kept the
Bcc: filter
and dumped most of the rest (actually it looks for messages that
don't
have my address in some *other* header line, ie, To: or Cc:).

I've only had a couple of false positives, and none were on the
Bcc:
filter-- Bcc: mail almost never comes from an *unknown* source.
Of course I
have to turn the filter off temporarily any time I subscribe to

a mailing list, until I can see a couple of sample messages and find something in the header for the filter to look for.

The real risk is letting someone else define spam for you, without explaining their methods.

(Do they have an option to automatically accept e-mail from anyone in your address book file? Or to build some other kind of exception file? Seems like an obvious thing to do...)

✉ Re: Junk-mail filters (Cattarin, [RISKS-20.89](#))

"Ray Todd Stevens" <raytodd@kiva.net>
Sat, 3 Jun 2000 19:09:57 -0500

It sounds to me that a need feature is missing for the filtering. It would seem that an important question for this type of filtering is "is this someone I e-mail a lot". Maybe this is a risk of building very complicated systems on top of a weak foundation.

Ray Todd Stevens, Senior Consultant, Stevens Services, R.R. # 14
Box 1400
Apt 21, Bedford, IN 47421 (812) 279-9394 Raytodd@tima.com

✉ Re: Junk-mail filters (Cattarin, [RISKS-20.89](#))

Markus Peuhkuri <puhuri@ws18.tct.hut.fi>
31 May 2000 15:42:46 +0300

While automatic junk mail identification would be useful, I can't recommend word based filtering because of too many false positives. Swedish for "six" (i->e) can be a bit problematic word. Maybe they should use "five and one more".

A few years ago I lost some US\$20 because of Subject-words filter; (the mail was stored in a junk folder which I checked every now and then -- too late in that case).

Currently, I do filtering based on To: and From: fields

- * mail must be addressed to some of my addresses (mail list traffic is separated before)
- * sender must be someone I know (I've sent mail to)

If both conditions are satisfied, then mail is accepted to my primary inbox, otherwise it is put in low-priority folder.

Markus Peuhkuri ! <http://www.iki.fi/puhuri/>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 91

Thursday 8 June 2000

Contents

- [White House admits over one year of VP's e-mail lost forever](#)
[Doneel Edelson](#)
- [Julia Roberts wins control of her net name](#)
[NewsScan](#)
- [Dot-Com nightmare -- domain-name hijacking](#)
[NewsScan](#)
- [Cyber pirates](#)
[NewsScan](#)
- [UPS kills power](#)
[Daniel Norton](#)
- [Ford Explorers recalled due to "lock-up"](#)
[Alex Wiebe](#)
- [Re: "Incompatible software" blamed for phone-book fiasco](#)
[Malcolm Pack](#)
[Kevin Parker](#)
- [Bloat Dissections II](#)
[R.A. Downes](#)
- [Re: How not to distribute white papers](#)
[Ian Goldberg](#)
[Stanley Chow](#)
[Paul Wallich](#)

- [Re: Trash Compactor](#)
 - [Bernard W. Joseph](#)
 - [Robert Alberti](#)
 - [Bob Dubery](#)
 - [Re: India piggybacking on railway controls](#)
 - [Ramjee](#)
 - [Douglas W. Jones](#)
 - [Bcc: filtering vs spam - almost risk-free](#)
 - [Charles Arthur](#)
 - [Bob Jewett](#)
 - [Fredrik Staxaeng](#)
 - [Re: Blocking e-mail on headers](#)
 - [William Colburn](#)
 - [Y2K bug still manages to bite after five months](#)
 - [Paul van Keep](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✉ **White House admits over one year of VP's e-mail lost forever**

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

Thu, 8 Jun 2000 15:45:35 -0400

The details are that when a contractor migrated the server for the Office of the Vice President (OVP) to NT 4, a new partition was created, an E: drive, in order to have the standard IS&T configuration (Information Systems and Technology division of the Office of Administration), and this drive was not added to the OVP backup schedule. This drive contained the OVP e-mail files. The migration was done in April 1998 and the problem was discovered by IS&T staff in May 1999.

The full document is at:

<http://www.house.gov/reform/letters/00.06.07.wh.pdf>

🔥 Julia Roberts wins control of her net name

"NewsScan" <newsscan@newsscan.com>

Thu, 01 Jun 2000 07:33:01 -0700

Actress Julia Roberts has won control of the Internet name `www.juliaroberts.com`, after an international arbitration panel ruled that an accused cybersquatter had no legitimate interest in that name and registered it in bad faith. The World Intellectual Property Organization, which is one of four designated arbitrators of Internet domain name disputes, cited evidence that the defendant, Russell Boyd, had registered names of several famous movie and sports celebrities, and had even tried to auction the Roberts address on eBay. In reaching its quick decision, the panel is demonstrating its willingness to extend protection to famous individuals, even if they haven't formally registered their names as trademarks. [*Wall Street Journal*, 1 Jun 2000; NewsScan Daily, 1 June 2000: <http://interactive.wsj.com/articles/SB959810376180166493.htm>]

[NewsScan Daily is underwritten by IEEE Computer Society and Arthur

Andersen, world-class organizations making significant and sustained

contributions to the effective management and appropriate use of

information technology. NSD is written by John Gehl and Suzanne Douglas,

editors@NewsScan.com. NewsScan items are reproduced in RISKS with permission. PGN]

🔥 Dot-Com nightmare -- domain-name hijacking

"NewsScan" <newsscan@newsscan.com>

Fri, 02 Jun 2000 08:12:05 -0700

At least two Internet companies recently suffered a dot-com's worst nightmare -- their domain names were reregistered without their knowledge, and all traces of their legal ownership were erased. Web.net, based in Toronto, and Bali.com of Hong Kong both have suffered crippling losses from the hijacking, which occurred last weekend. Sleuthing by Web.net's owners found that someone in Jakarta, Indonesia had sent a forged e-mail to Network Solutions, asking them to redirect all the site's e-mail and Web site information to a new location. He then requested that the registration, which had been recorded with Network Solutions in 1993, be transferred to a Toronto registrar, and asked them to switch the ownership to someone living in Hong Kong. In Bali.com's case, an investigation shows that the name now belongs to someone living in Madrid, Spain. "These are what I call A-class domain names," says Toronto Star columnist K.K. Campbell. "If the person collected 50 of these, they'd have \$5 million in assets they could afford to sit on for a little while until they're laundered and then resold."

[*Toronto Star 1 Jun 2000; NewsScan Daily, 2 June 2000:

http://www.torontostar.com/editorial/updates/top/20000601NEW01d_CI-DOMAIN1.html]

⚡ Cyber pirates

"NewsScan" <newsscan@newsscan.com>

Mon, 05 Jun 2000 09:01:10 -0700

A company called Havenco has built what it calls a "data haven" on an abandoned military platform in the sea, six miles off Britain's coast, in order to offer communications services to clients who want to avoid monitoring by governmental authorities. Declaring his small fortress a sovereign country beyond the reach of British law, Havenco co-founder and chief executive Sean Hastings, a 32-year-old U.S. citizen, says, "Technology has made it easier to move information and hide information. Soon it will be impossible to trace where money is and who has money, and that will eventually force governments to move away from income taxes and toward consumption taxes." [*The New York Times*, 4 Jun 2000; NewsScan Daily, 5 June 2000:
<http://partners.nytimes.com/library/tech/00/06/biztech/articles/04have.html>]

⚡ UPS Kills Power

Daniel Norton <danorton@chsw.com>

Wed, 07 Jun 2000 09:20:39 -0400

I received this over the weekend:

>Sunday, June 04, 2000 - 9:51:44 AM
>[We] would like to apologize for any inconvenience caused by
our brief
>outage on Sunday, June 4. A UPS backup system burned out,
cutting off
>power to some of our systems. Ironically, it is the UPS's job
to make sure
>that our systems HAVE a constant power supply, so this problem
was
>unexpected, and something we would not normally anticipate.
Thankfully,
>one of our systems administrators who was on call noticed the
problem and
>went onsite to rectify the situation.
>Thank you for your patience

As it turned out, my own systems automatically paged me within
20 minutes of
the failure. Why did they need someone to "notice" the problem?

Daniel Norton

⚡ Ford Explorers recalled due to "lock-up"

"Wiebe, Alex" <AWiebe@online-can.com>

Tue, 6 Jun 2000 08:46:18 -0500

Here's the link:

<http://cbc.ca/consumers/market/recalls/reclfull/2000/06jun2000b.html>

The title is shocking: Ford recalls Explorer due to air bag
problems

The body is mildly humorous for those who can envision the slap
stick comedy
routine that could result from "An inoperative front windshield
wiper system
could adversely affect driver visibility." Looks like a bit of

electrical

noise can cause some central computer to lock up, the result is anything ON

will stay ON, anything OFF will stay OFF.

The risks are: There is no mention of the air bag in the article. Was this

an eye catching hook? or was some critical detail left out of the article.

Electrical noise locking up a computer? This is a problem as old as

transistors - maybe older. A vehicle is a very noisy place, hopefully the

[engine]ers who let this slip get their hands slapped.

Alex Wiebe, Online Business Systems - (204) 982.0200

Voice: (204) - 982.0322 awiebe@online-can.com

⚡ Re: "Incompatible software" blamed for phone-book fiasco **(RISKS-20.90)**

Malcolm Pack <risks@potnoodle.net>

Mon, 05 Jun 2000 23:06:34 +0100

I received this from a San Diego resident. I'll post it verbatim, because it will hopefully raise a smile, even if it doesn't add to your knowledge of the matter...

| BTW, have you hoid about the fiasco/brouhaha here in sunny Southern

| California? The fruits and nutz are alive and well. Picture this...

| Sicily, 1945... no wait!

|
| Cox Communications, the local cable TV monopoly ain't making enuff money

| on cable TV, so dey spread out (SPREAD OUT!) into being an

ISP. Dat's

| nice. Are they happy having money raining down on them faster
then they

| can count it?

| OF COURSE NOT! So, what better idea then to SPREAD OUT! into
providing

| phone service too!

| So far, so good. Now the fiasco...

| It seems CoxPhone needs to send in their phone subscribers'
names/addresses/phone numbers to Pacific Bell aka PacBell.

| Well, it seems Cox sent in *all* their phone subscribers' n/a/
#s,

| including the folks paying extra for unlisted numbers. PacBell
prints

| the phone books and starts distributing them. 400k of 1.3 mil
phone

| books were distributed before someone, like a Cox phone
subscriber hits

| the roof when s/he finds out their 'unlisted' number is listed.

| Quick like a bunny, Cox calls PacBell to STOP DA PRESSES!

| PacBell sez, no problem. Now it seems they can't get together
to figure

| out what to do. Junk the phone books they have left, retrieve
the 400k

| they distributed, who pays for what, etc. PacBell is going to
| distribute the rest of the phone books as they don't want to

lose

| advertising dollars and it wasn't their problem that they
didn't

| notice Cox's database of names include unlisted numbers.

| Anyways, we'll have everyone suing each other while Cox and
PacBell

| claim a 'computer error' for the problem. So it wasn't their
fault.

| Everyone is nuts here! Must be sunstroke or the bottled
water, IMO.

Malc, Southend-on-Sea, UK

**⚡ Re: "Incompatible software" blamed for phone-book fiasco
([RISKS-20.90](#))**

Kevin Parker <sophist@rocketmail.com>

Mon, 05 Jun 2000 15:02:57 -0700

An interesting story concerning the Cox/Pac Bell unlisted phone number fiasco.

When I got the new phone book a few weeks ago from Pac Bell, I thought I'd look up an old acquaintance from high school to see if he was listed. Not only was he listed, but he lived in our housing development, two doors down from friends of mine. The next time I went to visit the friends, I stopped by to see if John was home. A woman and some kids were out front, so I asked her if John C. lived here. "Why do you want to know," she said. I knew him in high school, I replied. "What's your name?," she wanted to know. I told her. She then asked me how I got their address. I told her that it was in the new Pac Bell phone book. Impossible, she said, since ours is an unlisted number. Well, I told her, not only is your phone number printed, but so is your address. She became really concerned and said, "This is not good. John and I are both police officers, and John works undercover. He can't have his name published."

A few weeks later the **LA Times** mentioned the snafu.

[The risks of this episode run deep. PGN]

✦ Bloat Dissections II (Re: [RISKS-20.35](#))

R.A. Downes <root@radsoft.net>

Mon, 05 Jun 2000 15:01:05 +0000

The bloat dissections continue. One remaining question in the article cited above and its follow ups is: "would dissecting such an application as RegClean at source level really reduce its bloat?"

Curious coincidence then, that I should happen upon the source code to another Microsoft Registry cleaner - RegMaid, from 1993 - 95 (btw, this application might very well be the basis of the later RegClean project as well, judging from the embedded resources).

Fact: the distributed executable to RegMaid is 153,600 bytes.

Fact: it is distributed with its source code.

Fact: after less than ten minutes work I got it down to 69,632 bytes.

This is a savings of 83,968 bytes, or well over half the original image size. This is a new image only 45% the size of the original. And in less than ten minutes. I got 83,968 bytes of bloat off my disk that fast.

Not to beat the dead horse but - just think about it. Ten minutes, 55% savings of 83,968 - and I had never seen this code before in my life.

If this doesn't prove that bloat is inexcusable, I'll just have

to send more examples. Cutting the bloat in that application, and attempting to estimate the cost of doing so, really misses the point too: the code itself is rather intricate, and this Rome was not built in a day. Barring the author's getting the architecture completely right from the beginning, the ten minutes it took to shave the EXE by 55% represent:

1. Half of only one coffee break.
2. A late arrival into the Thursday night Quake game.
3. One final tweak in the evening before dinner is really served.
4. Something to do on the laptop while commuting to work in the morning.

It's **trivial**. Avoiding bloat has never been an effort, despite what the defenders of latter-day commercial software like to claim. Things can be done right from the beginning, or even if not, corrected in a negligible envelope of time.

As for really astounding comparisons, try:

http://radsoft.net/bloatbusters/sw_dns.htm

Where we got a monster down from 3.5MB to just 7KB (seven kilobytes) in a single hour!

It's professional pride on the one side -- and "who cares?" on the other.

RA Downes <radsoft.net> <http://radsoft.net>

🔥 Re: How not to distribute white papers (Re: Rubin, [RISKS-20.90](#))

Ian Goldberg <iang@cs.berkeley.edu>

Mon, 5 Jun 2000 14:44:45 -0700

Actually, the "unzip" program available for Linux (as well as, I assume, the equivalent unzip programs for Windows) is able to decompress these self-expanding archive programs.

So there's no need to actually run the .exe file (which is good, since I don't **have** a Windows box on which to do so, anyway).

Of course, once we do that, we discover that it expands into a Microsoft Word file...

- Ian "Yes, I know about wvWare."

[Similar comments from several others. TNX! PGN]

✶ Re: How not to distribute white papers (Re: Rubin, [RISKS-20.90](#))

Stanley Chow <stanley.chow@cloakware.com>

Tue, 06 Jun 2000 14:48:32 -0400

Avi Rubin ([RISKS-20.90](#)) talked about the difficulty of using "sacrificial" machines for quarantining potential malware.

The latest release of VMWare (see <http://www.vmware.com>) has some useful features for this purpose. One can set up a virtual machine to have the desired O/S, patches, products, etc, then take a snap shot. You can then just copy a new virtual machine and throw it out after. (There are some path settings that have to be done, but I wrote a perl script). They

also allow
the disk to roll back, very cool.

Note that my relationship to VMware is purely as a customer.

Stanley Chow VP Engineering stanley.chow@cloakware.
com
Cloakware Corp (613) 271-9446 x 223

⚡ Re: How not to distribute white papers (Re: Rubin, [RISKS-20.90](#))

Paul Wallich <pw@panix.com>
Tue, 6 Jun 2000 09:33:33 -0400

Microsoft is more likely doing this to restrict distribution of
the text
file as it sees fit. The same savings of space could be achieved
simply by
delivering a zipped file and letting the user's software
recognize the MIME
type for decompression. Bundling the file into an executable,
however,
arguably meets the requirements of the Digital Millennium
Copyright Act for
a technological copy-protection mechanism, which makes
unauthorized
redistribution of the text a serious crime (where "serious"
means "you could
go to jail for more than a year").

I don't know if that particular white paper (or the page from
which it was
downloaded) contained a license agreement restricting
redistribution of the
text, but if it did, that would certainly appear to meet the DMCA
requirements. (This kind of thing has already bitten other
ostensibly open
MSFT documents.)

Indeed, depending on the state from which you accessed the document (or in which the server was located) UCITA might apply as well, in which case you could have to check the download page for links to any agreement governing use of the document, and recheck at regular intervals should MSFT decide to restrict the text in the future...

> I could not believe that this is how Microsoft
> distributes its white papers. It is beyond comprehension.

If you view control, rather than dissemination, as the goal of putting documents on a web site, it's easy to comprehend.

Paul Wallich <pw@panix.com>

🔥 Re: Trash Compactor ([RISKS-20.90](#))

<bjoseph@mail1.industry.net>
Thu, 08 Jun 2000 09:40:26 -0400

In [RISKS-20.90](#), Robotech_master wrote about a thief jumping into a weight-activated trash compactor. I live here where it happened and attest that the story was the first one that went over the wire services. As the story developed, new facts indicated that it was a garbage truck into which she jumped, and that the workers manually activated the compactor. That didn't make the wire services.

In his book Fables for Modern Times, James Thurber said, "He who hesitates is sometimes saved." The news services probably should not have

been so
eager to publish before all the facts were known;
Robotech_master probably
should not have jumped on the story as a risk; I probably should
not have
answered.

Bernard W. Joseph <http://bbs.industry.net/html/bjoseph>

[Also noted by Vincent Dovydaitis, in
[http://dailynews.yahoo.com/h/ap/20000601/us/
brf_compactor_death_3.html](http://dailynews.yahoo.com/h/ap/20000601/us/brf_compactor_death_3.html)

Hesitates? The object of the media is to sell their wares.
*The New

York Times* meticulously publishes corrections on Page A2 each
day.

Not everyone else is as careful. But RISKS tries very hard to
correct

the record, although if we waited for verification on such
items,

the wait would be very long... Incidentally, the risk of a
hyperactive

automated compactor still remains a risk. PGN]

✉ Re: Trash Compactor ([RISKS-20.90](#))

<Robert.Alberti@born.com>

Wed, 7 Jun 2000 11:25:27 -0500

Two AP follow-up articles state that the compactor was not
automatic, but

was started by employees while the woman was inside.

Unfortunately for her,

the employees were apparently deaf...

<http://detnews.com/2000/metro/0006/01/d02-66693.htm>

[http://www.detroitfreepress.com/news/statewire/sw13442_20000531.
htm](http://www.detroitfreepress.com/news/statewire/sw13442_20000531.htm)

Robert Alberti, BORN Security Practice Lead <Robert.Alberti@born.com>

⚡ Re: Trash compactor kills shoplifter ([RISKS-20.90](#))

"Bob Dubery" <bdubery@netcare.co.za>
Tue, 6 Jun 2000 08:31:05 +0200

Surely when designing such a device, one is entitled to not have to cater for the fact that people may use the device for something that it is not designed for?

I recently had someone tell me that a light fitting on the external wall of my house was a risk because somebody could get a shock from it. I replied that yes, somebody could, but only if they were trying to remove it - in which case they probably deserved the shock.

Everyday I see indications that people are less and less inclined to take responsibility for their own stupidity or, in some cases, dishonesty. The risks to society of that attitude far outweigh the risks posed by automated hardware that doesn't cater for the whims of every turkey that walks down the street.

⚡ Re: India piggybacking on railway controls (Bakowski, [RISKS-20.90](#))

<sramjee@hss.hns.com>

Wed, 7 Jun 2000 17:33:44 +0530

Actually the guy called Ashok Jhunjhunwallah who is spearheading the efforts is a respected professor from IIT Madras and is working for the promotion of indigenization of technologies. He has been working with WILL and DSL on Cu for a while now... He has been reasonably successful so far.

Moreover, the fact is that the railway stations are interconnected for normal voice traffic thru quad Cu cable. As a matter of building in a possible onfail crossover and to control the trains in future by some means, there is also a spare cable (running parallel to the whole system) which is *not at all* used. Ashok and friends want to make use of this spare, to start with, to operate a railway based Internet backbone n/w. And later, they are planning to factor in the spare capacity of the railway's fibre optic n/w as also by laying fresh cables. The spare cable will be used for high bit rate data link and WILL will / could be used in hubs at railway stations etc. Actually it looks like an elegant and pragmatic solution, political will permitting...

This much said, I don't think there is a risk associated with this as the trans modes are not at all going to interfere with the existing comm systems for the management of Indian railways...

But don't you think, it will be easier to "train" our guys to use the Internet this way? ;-)

--ramjee

⚡ Re: India piggybacking on railway controls (Bakowski, [RISKS-20.90](#))

Douglas W. Jones,201H MLH,3193350740,3193382879 <jones@cs.uiowa.edu>
5 Jun 2000 22:13:08 GMT

No, this looks exactly like the way the Sprint long distance carrier got its service. Consider the expansion of the acronym:

Southern Pacific Railroad INternal Telecommunication

(recalled from memory, so it may only be approximately correct.) This company was founded to sell exactly the kind of excess bandwidth that the Indian railways are interested in exploiting, and there's no evidence that use of surplus capacity in lineside cables leads to trouble.

Doug Jones <jones@cs.uiowa.edu>

⚡ Bcc: filtering vs spam - almost risk-free (Bean, [RISKS-20.90](#))

"Charles Arthur, The Independent" <carthur@independent.co.uk>
Tue, 6 Jun 2000 10:36:55 +0100

> My log files showed that 96% of the spam was being deleted by the Bcc:
> filter and not even getting to the "clever" ones.

That has been exactly my experience (I had 95%).

I can't understand why Microsoft introduced content-based filtering. This is sure to be (1) slower (2) less accurate. The unique thing about spam is not its content, which can be just about anything, but the fact that it's, well, spam, and hence not aimed at you.

Some spam programs do do individual addressing: these are the annoying 5% which elude the Bcc filter. For anyone who may expect to receive e-mail from people they've never met (such as journalists like myself) though, you can't just trash stuff on that basis.

From being a major annoyance though, spam has become a minor irritation via Bcc filtering. It is now the only spam filter I use. (After other filters looking for stuff from mailing lists have done their work.)

Maybe MS couldn't copyright Bcc filtering?

✂ **Bcc: filtering vs spam - almost risk-free (Bean, [RISKS-20.90](#))**

Bob Jewett <jewett@netcom.com>

Mon, 5 Jun 2000 21:08:07 -0700 (PDT)

In [RISKS-20.90](#) Ron Bean remarks that his Bcc: filter had few false positives. That filter is also used by many here, but that may have to change. There is now circulating a "Use BCC or be assaulted" hoax. The summary from <http://www.snopes.com/horrors/mayhem/bcc.htm> is:

"Woman is stalked by on-line acquaintance; use the "blind carbon copy" feature in e-mail to prevent this from happening to you!"

I am seeing increasing numbers of mailing list submissions which have no valid To: or Cc: address. Is it just ignorant users who have stumbled onto mailer features? I fear that they fear the above. I got the hoax in e-mail from the usual (fearful) person who sends me hoaxes. Did a spamster start the hoax?

Bob Jewett

⚡ **Bcc: filtering vs spam - almost risk-free (Bean, [RISKS-20.90](#))**

Fredrik Staxaeng <fstx@algorithmica.se>
Wed, 7 Jun 2000 18:46:08 +0200 (CEST)

Any junk-mail filter made by Microsoft will soon have a 100% false positive rate. The spammers will check that their message passes the filter.

Fredrik Stax\ang | fstx@algorithmica.se | (+46) 8 678 09 94

⚡ **Re: Blocking e-mail on headers ([RISKS-20.90](#))**

Schlake (William Colburn) <schlake@nmt.edu>
Mon, 5 Jun 2000 21:24:01 -0600

I define a lot of anti-spam here for my users without them ever being aware of it. I am always very careful about what I block, and I get e-mail summaries of the messages every day (which I actually look at every

weekday). In addition to my own anti-spam, I also include pieces of Eric Allman's anti-spam from the knecht.mc file. Eric uses a rule that blocks "friend@" and "@public.com" in the "To:" field. If Eric Allman uses it, then it is good enough for me, or so I thought.

Turns out that there is someone out there with a real last name of "Friend". His e-mail address was "friend@<somewhere>.edu", and mail from us to him was being blocked. I modified the rules to check for the specific case of "friend@public.com" in the "To:" line instead of "friend@anywhere" and "anyone@public.com". Then I contacted the guy whose e-mail I had blocked, and told him all about why his e-mail had been blocked.

He was most grateful to me, and said that he had a lot of e-mail disappear all the time, and then he changed his account name. The risk here, is that automated processes can chug along for years without anyone ever noticing that they are broken. Poor Mr. Friend may have been silently losing e-mail for years, and could still have been losing e-mail today if it hadn't been noticed at my end. There is also a risk in someone trying to plug in someone else's solution. Eric Allman's personal machine is a lot different than my mail server with 3000 users on it.

<http://www.nmt.edu/~schlake/>

⚡ Y2K bug still manages to bite after five months

Paul van Keep <paul@sumatra.nl>

Thu, 08 Jun 2000 17:28:40 +0200

To my amazement I was hit by a Y2K bug last week. Last Wednesday I was in Chalon-sur-Saone at a pickup point from La Redoute, a french mail order company. I was there to collect an order and pay for it. And that's where things went wrong. The clerk tried to enter my credit card into their computer system, but it kept refusing it, claiming the account was blocked (not the card.) Of course it took her a couple of tries before she realized that the problem wouldn't disappear by itself. So she called their head office in Roubaix to ask them to unlock the account. It took two long phone calls but in the end my card was accepted and I could pay for the goods. When I asked her why my card was rejected she said it was caused by a Y2K problem. Their computer system stores a maximum of two credit cards in an account profile. This is, as we all know, a big risk in itself. It simply means that my card information is available to anyone at La Redoute who has access to their customer system. In my case, two card numbers were stored, both my wife's and mine. But when they converted their system to be Y2K compliant the process erased a number of expiration dates including that of my wife's card and probably mine too, both being 06/00. When I tried to pay with my card, the correct expiration date was entered into the system again, but my wife's card number still had a blank date connected to it. So the system decided to block the account. There are two extra risks besides the

obvious one of storing credit card information: wiping valid data while trying to clean up a database for a Y2K conversion and being overprotective when checking account information.

Paul van Keep



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 92

Friday 16 June 2000

Contents

- [Grade fixing](#)
[PGN](#)
- [Jury blames computers for Cali plane crash](#)
[Scott Lucero](#)
- [Black boxes, telemetry, and autopsy](#)
[Lord Wodehouse](#)
- [For want of \\$35, J.P. Morgan loses its Web site and e-mail](#)
[Keith A Rhodes](#)
- [Another example of systems that don't talk to each other](#)
[John Pettitt](#)
- [Bad background checks on Slashdot](#)
[Michael D. Crawford](#)
- [No password recovery on B2B WWW site](#)
[Dirk Bank](#)
- [JustBeFriends for macro virus control](#)
[Gary McGraw](#)
- [Re: Bloat Dissections II](#)
[Martin Ward](#)
[Graham Mainwaring](#)
[Edward Reid](#)
[Nevin Liber](#)

● [Re: Indian Railway Fiber](#)

[Jay R. Ashworth](#)

[Chuck Charlton](#)

[Bart van Leeuwen](#)

[James Ryan](#)

● [REVIEW: "Information Hiding Techniques for Steganography and Digital Watermarking](#)

[Rob Slade](#)

● [Call For Participation - RAID 2000](#)

[Herve Debar](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ **Grade fixing**

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

Thu, 15 Jun 2000 9:02:47 PDT

At least 20 Berkeley High School seniors (hopefully, graduating) are

apparently involved in a grade altering episode. The grade program is

accessible to only about 20 employees, who must use **two** passwords. (Wow,

that is REAL security!) But one of the computers was most likely left

logged in and unattended. One student admitted paying \$10 for the change.

[Source: article by Meredith May, **San Francisco Chronicle**, 15 Jun 2000, A26]

⚡ **Jury blames computers for Cali plane crash**

"Scott Lucero" <LuceroDon@hq.optec.army.mil>

Thu, 15 Jun 2000 14:09:04 -0400

A US federal jury today found that an aviation computer software company and a flight-computer manufacturer contributed to the 1995 crash of an American Airlines jetliner in near Cali, Colombia. 159 out of 163 passengers were killed. The jury said Jeppesen was 17 percent responsible, Honeywell 8 percent at fault, and American Airlines 75 percent responsible.

Honeywell attorneys believe the pilot guessed by punching in the first of 12 options for navigational beacons sharing the code letter R instead of the correct code "Rozo", which would have carried the jet straight down a valley into Cali. The first "R" turned the jet toward Bogota, and the intervening mountains.

It turns out that 95 of 8,000 navigational beacons worldwide were not coded in the database as beacons. "Rozo" was stored in another file.

Apparently, Jeppesen understood the risks. 11 months before the crash, one of their memos states: "The situation with this group of navigational aids has reached a boiling point. We will have to act now to meet our customer needs."

Another unfortunate example of the risks of doing nothing when safety critical problems surface.

<http://abcnews.go.com/sections/travel/DailyNews/Software000613.html>

Scott Lucero

✶ Black boxes, telemetry, and autopsy

Lord Wodehouse <w0400@ggr.co.uk>

Fri, 14 Apr 2000 10:27:34 +0100

Watching a few nights ago on Channel 4 in the UK, I saw a programme called Equinox on flight data recorders (black boxes) and the "failures" of these to identify the cause of accidents, especially when only recording a few parameters. The case against Boeing was put, when the company adopted a different interpretation of the data, because not enough points were available to actually determine exactly what happened at certain times. This is all somewhat emotive as it was connected with the 737 rudder deflection crashes.

However one view put forward was that real-time telemetry would ensure that potential problems could be spotted as they happen and this would move the problem of crash investigation from autopsy mode to crash prevention.

I myself remain unconvinced. For a start to get all the real-time data logged and monitored would be a huge effort, requiring lots of technology and be expensive and hence resisted. Secondly when a problem strikes, although the pilot may have incomplete or no information about the cause s/he is the person up there where the problem is. The ground monitoring staff will only see one side of the issue and I can see a conflict between their views and the flying crew. Telemetry may well work well for the USN and test pilots or for space missions like Apollo (13 in

particular), but when there are so many planes flying, will it really work as well? Any failure to get the real-time data could also lead to issues of whether a plane half-way across the ocean should fly on or turn back.

However British Airways does have a system of recording lots of aircraft parameters on recorders on the flight deck. The tapes are played back after the flight to see if issues occurred and to monitor the state of the plane. This seems to be a way of spotting problems and following trends, so that fault prediction can be done and the risk of crashes reduced.

Planes will always crash, often due to human error and almost always due to unforeseen circumstances. By ensuring that the flight data recorders store enough data and that a quick access means such as a separate data recorder in the cockpit is available so data is collected easily from each flight, it will be possible to reduce the accidents and provide a better chance of uncovering the cause. Relying on technology like real-time telemetry to be a magic bullet is folly.

Global Research Information Systems, Glaxo Wellcome Medicines Research Centre
Gunnels Wood Road, Stevenage SG1 2NY UK +44 1438 76 3222
w0400@ggr.co.uk
<http://ds.dial.pipex.com/lordjohn/> and <http://www.lordjohn.demon.co.uk/>

⚡ For want of \$35, J.P. Morgan loses its Web site and e-mail

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

Wed, 14 Jun 2000 09:35:43 -0400

J.P. Morgan & Company (worth \$21 billion) lost its Internet connectivity on 13 Jun 2000 because they failed to pay their \$35 bill from Network Solutions for their jpmorgan.com domain: three bills ignored over six weeks. All of their Net customers were affected. (Last year Microsoft failed to reregister a domain name necessary for Hotmail service, although a computer consultant bailed them out by paying the fee for them.) [Source: Article by Patrick McGeehan, 14 Jun 2000; PGN-ed]

⚡ Another example of systems that don't talk to each other

John Pettitt <jpp@cloudview.com>

Mon, 12 Jun 2000 12:08:33 -0700

CobraServ (a service company that handles health insurance payments) sent me a "you didn't pay so we're going to cancel you" letter dated June 7th. Yet when I call their automated voice response system it happily tells me that my last payment was received June 5th! Almost makes me want to go back to the British National Health Service.

⚡ Bad background checks on Slashdot

"Michael D. Crawford" <crawford@goingware.com>

Thu, 15 Jun 2000 15:01:54 -0700

The story "When Background Checks Go Wrong" on <http://slashdot.org> at

<http://slashdot.org/article.pl?sid=00/06/07/211250&mode=thread> is about someone who couldn't get a job because of a mistaken felony arrest that appeared on her record, and discussion of liability for the employers and private investigators.

Many, many people weigh in on the commentary with their own experiences with mistaken background checks, and I post my own experiences in being mistaken for other Michael Crawford in the same schools, at the same companies, and in the arts (hint: I didn't star in Phantom of the Opera).

BTW, I try to refer people to Risks sometimes on Slashdot. I think it would be helpful if more risks readers would post on slashdot and refer the readers to relevant issues of Risks. Slashdot is a very high-visibility site in the open source community and I think they could use the sober realizations that come from reading risks when writing more open-source code.

Michael D. Crawford crawford@goingware.com <http://www.goingware.com>

⚡ No password recovery on B2B WWW site

Dirk the Daring <dirk@psicorps.org>
Mon, 12 Jun 2000 18:23:16 -0400 (EDT)

I work for a large, multinational telecomm and computer firm based in the western USA. We have a standing contract with a large US-based printing and stationery firm to produce all our stationery, letterhead, business cards, etc.

Having recently obtained a number of industry certifications (something I studiously avoided doing for the past 15 years, but I now find myself employed by a company which cares about these), I decided it was time to update my business cards to reflect these certifications.

I followed the links from our company intranet site to the printing firm's B2B site where we can order such things. I was prompted for some information, including my Human Resources ID (HRID) and password. Well, its been two months since I ordered anything, so I'd forgotten my password. They offered a helpful "Lost your password?" link, which led me to another screen where they asked from the E-Mail address I had used. I tried all my E-Mail addresses, none of them were accepted by the system as a valid E-Mail address to send a password to.

OK, fine. I called the toll-free help #, and spoke with a nice woman. I explained the problem to her, and she immediately grasped it. She suggested that I return to the main page and enter a whole new record, using a new (fake) HRID.

This seemed redundant to me - I already had a valid system record with all my demographic information, and I wasn't enthused about re-entering all that

information. Couldn't she just reset the password? No, she explained, she had no access to that, and had no idea who did. The only way for me to get back in would be to totally re-create my user profile, using a faked HRID.

Risks: B2B e-commerce is great, but systems need to have competent human backups. The help phone # was basically the printer's sales line. The staff there knew about the WWW site, but had little technical information on it.

Too, if HRIDs can be faked, then its child play for anyone to get business cards showing them to be employed by my company, whether or not they are actually employees.

Finally, there as only one mechanism for triggering the forgotten password service, and that was based on E-Mail address. However, the system evidently keyed its records on HRID, because when I re-created my user profile, everything was the same as I had previously entered, except for the fake HRID (when I originally tried to re-create my user profile, I used my actual HRID, and it told me the record already existed). There's no good reason to my mind that the system should key off of HRID but use the E-Mail address for triggering the forgotten password service.

In all, I found this printing company's B2B WWW site a good example of how NOT to implement B2B services.

Dave Bank dirk@NOSPAM.psicorps.org

⚡ JustBeFriends for macro virus control

Gary McGraw <gem@rstcorp.com>

Wed, 14 Jun 2000 16:48:11 -0400

Reliable Software Technologies has just released a new program (JustBeFriends) designed to prevent e-mail macro viruses from spreading. It can be used along with or instead of the Microsoft supplied e-mail protection patch. JustBeFriends works with all versions of Outlook and Outlook Express, and is substantially simpler than the Microsoft patch. For full details, see <http://www.rstcorp.com/news/jbf.html>.

E-mail viruses spread by exploiting existing mail programs to send themselves to a large number of new recipients. In addition, many viruses may also modify or damage the computer on which they are run. While most home and office computers are not sufficiently secure to make preventing damage to files on the computer possible, it is possible to make sending e-mail from scripts much harder. This move limits a particularly nasty way that viruses propagate. Both Microsoft's security update and JustBeFriends succeed in disabling script-based e-mail.

Microsoft's approach works by internally controlling access to a large number of subsections of Outlook that can be used to gather e-mail addresses or send e-mails. Unfortunately, in order to prevent future e-mail viruses, this list of protected objects needs to be exhaustive. E-mail addresses may still be exposed if they appear in signatures, message bodies,

or other documents. Future methods for exploiting flaws in Outlook to send e-mails are likely to be found.

JustBeFriends works by controlling the ability of other applications to access Outlook or Outlook Express. In the event that the access comes from a script being run from the desktop or from an attachment, the access is denied. Otherwise, the user is asked to confirm that the application should be allowed access to Outlook.

JustBeFriends was developed primarily by Tim Hollebeek, Research Associate at RST Labs. It makes use of advanced technology developed in part under a DARPA grant titled "Sandboxing Mobile Code Execution Environments".

🔥 Re: Bloat Dissections II (Downes, [RISKS-20.91](#))

Martin Ward <Martin.Ward@durham.ac.uk>

Fri, 9 Jun 2000 10:12:54 +0100 (BST)

Someone at our company wrote a short MS Word document (just a handful of pages) and e-mailed it, as an attachment, to several people in the company. The document contained several screenshots. For some reason, MS Word stores these images in a **completely** uncompressed format. The result was a 20Mb document which expanded into a 26Mb e-mail message. This message was too big to be delivered via modem: the pop3 server kept timing out after

about 20Mb worth.

The kicker is that when I finally downloaded the document via a fast internet connection and ran gzip on it, it compressed down to just 180Kb! That's a factor of over 100 to 1 compression from just a few seconds of effort.

With just a few mouse clicks you can bloat your word document to multi-megabyte network-spamming size and send it to hundreds of mail boxes. There are any number of lossless image compression formats, plus any number of general purpose file compression algorithms, any of which would make a huge improvement. Even the dumbest run length encoding would make a big difference on a screenshot. But Microsoft just doesn't care:

- (*) Their image file format doesn't compress images;
- (*) MS Word doesn't compress files when it stores them;
- (*) E-Mail attachments are not compressed.

As RA Downes says:

> It's professional pride on the one side -- and "who cares?" on the other.

Martin.Ward@durham.ac.uk <http://www.dur.ac.uk/~dcs0mpw/>
Maintainer of the G.K.Chesterton web site: <http://www.dur.ac.uk/~dcs0mpw/gkc/>

✶ Re: Bloat Dissections II (Downes, [RISKS-20.91](#))

Graham Mainwaring <graham@mhn.org>

Fri, 9 Jun 2000 20:25:22 -0400 (EDT)

While I generally agree with Mr. Downes that software bloat is

undesirable,
unnecessary, and often quite easily prevented, I take exception
to the
manner in which Mr. Downes and Bloatbusters make their case.

For example, they do not use the same standards when measuring
the size of
their own code as they do when measuring the size of 'bloat'
examples. Bloatbusters claims their replacement for Solar Winds'
DNS
resolver is only 7k. In fact it also depends on MSVCRT.DLL, the
Visual C++
standard library, which is 288k. It would be reasonable to claim
that since
this file comes with Windows, it shouldn't be counted against
Bloatbusters'
totals - yet they count this file in totals where their agenda
calls for a
higher figure. The case against bloat is clear enough without
resorting to
this sort of accounting trickery.

I would also like to contest Bloatbusters' claims regarding the
Delphi
programming language. It is certainly true that if you naively
load Delphi
and create a project with a single form, you will link in a lot
of stuff you
don't need. The same is true of an MFC application in Visual C+
+. The
conclusion to reach is not that Delphi can only produce bloated
applications, but that bloat reduction requires skill on the
part of the
programmer.

Bloatbusters at one point refers to the size of a minimal
windows GUI
application, capable of displaying a window, closing itself, and
nothing
else. I have coded this application in both Visual C++ 6.0 and
Delphi 5.0.
In C++ it is 63 lines of code and a 24k EXE. In Delphi it is 59
lines of

code and a 17k EXE. (Source available on request via e-mail.)

These

applications are very much identical line-by-line, do not depend on any

external libraries or DLLs other than Windows itself, and behave identically. I believe these are the smallest possible self-contained

Windows EXEs sizes for each environment. If, as Bloatbusters' site claims,

"Delphi means BLOAT," then why is the Delphi app smaller?

However, having gone to the trouble of writing these applications, it occurs

to me that I am departing wildly from my normal style of programming in both

Delphi and C++. I have not actually coded a message loop in several years,

and would not expect to do so outside this contrived example. If I were

writing a GUI application of any complexity, it would be frightful to

consider writing it with nothing but C message loops and massive switch

statements. Not only would the initial development require much more

programmer effort, it would be far more difficult to maintain once

complete. Windows applications had to be written this way in 1988 because

there were no better tools. Today, I would consider it unforgivably

irresponsible to code this way.

Good management of software development risks is a very hard thing to do,

and certainly, excessive code bloat represents a real risk to eventual

maintainability and supportability. But it is not the only one or the most

serious one. Writing code in such a way that mid-level programmers inspect

and understand it in relatively short time periods is at least equally

risk-preventive. Sacrificing every other consideration for the pursuit of small EXE sizes is really not the right thing to do.

✶ Re: Bloat Dissections II (Downes, [RISKS-20.91](#))

Edward Reid <edward@paleo.org>

Sun, 11 Jun 2000 23:41:18 -0400

> Things can be done right from the beginning, or even if not, corrected in
> a negligible envelope of time.

On the latter, minor point I disagree. It is **not** always trivial to eliminate bloat once the program is written. Many times it is, but sometimes it requires serious reworking of the program.

Done properly to begin with, it's not only as easy to deflate as to bloat, in general it's easier just because it involves thinking ahead about the design. It's a good example of the old maxim "if you don't have time to do it right, where are you going to find the time to do it over?".

✶ Re: Bloat Dissections II (Downes, [RISKS 20.91](#))

"Nevin :-\] Liber" <nevin@enteract.com>

Fri, 16 Jun 2000 02:21:44 -0500

> This is a savings of 83,968 bytes, or well over half the original image
> size. This is a new image only 45% the size of the original.

And in less

> than ten minutes. I got 83,968 bytes of bloat off my disk that fast.

However, this ten minutes didn't include any regression testing so you could have at least some confidence that your refactoring of the code didn't break anything, let alone enough confidence to ship it knowing that there is 100% backwards compatibility (and willing to put your reputation and/or money on that guarantee).

The real cost isn't in the 10-minute fix; it's in verifying the 10-minute fix. That is the RISK.

> If this doesn't prove that bloat is inexcusable, I'll just have to send
> more examples.

Like everything else in software, it is a tradeoff.

Let us look at the cost of hard drive space. A 20G drive can be gotten for \$170. That is \$8.5/GB which is less than 1 cent/MB.

Your fix is worth, at best, a fraction of a cent to your customer. If this causes you to slip shipping by even one day, you've made a bad decision to work on it.

Now there are places where code space isn't so cheap and this is worth doing. I've worked on projects in the past where reducing the number of floppies our product had to ship on was a significant cost savings. OEMs might want a smaller package to duplicate as they can increase the number of systems they can build per hour. Many embedded devices have a

limited

amount of ROM and RAM, and it is worth the effort to tighten the code up to get it to fit.

> It's professional pride on the one side -- and "who cares?" on the other.

That isn't it. It is about knowing when it is worth taking the RISK and

spending the time to reimplement working code and retest it.

All the best

software engineers that I know take their professional pride in making that

decision correctly as well as when they reduce the bloat.

Nevin ":-)" Liber <mailto:nevin@enteract.com> (773) 961-1620

✉ Re: Indian Railway Fiber (Jones, [RISKS-20.91](#))

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

Sun, 11 Jun 2000 16:59:56 -0400

> Southern Pacific Railroad INternal Telecommunication

I thought the N expanded to 'Network', myself, but...

Gee. Isn't anyone catching the *real* risk? Or do I just hang out on NANOG too much?

The problem with putting high-cap fiber next to railroad tracks is that the trains tend to fall off of them occasionally... and there's no good place to put the backup fiber, precisely because of the reasons you wanted to put the fiber by the tracks in the first place.

RISKS of assuming you've discerned all the RISKS?

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

⚡ Re: Indian Railway Fiber (Jones, [RISKS-20.91](#))

Chuck Charlton <chuckc@stanford.edu>

Thu, 15 Jun 2000 16:03:51 -0700

Sprint did indeed start out as the telecommunications division of the Southern Pacific Railroad, As Douglas Jones mentions, but with an important difference. By the time SP began to resell some of its capacity to other businesses, they were not selling wires or access to wires. They were selling capacity on Supergroup 2 in the microwave system that paralleled the tracks.

The acronym is suspect, also. When SP spun off the communications company, its official name was SP Communications for the first few years. It was only later that they changed the name to Sprint.

Chuck Charlton, Manager, Facilities Operations Work Support Center
650.723.5225 voice 650.723.0823 fax 650.867.8057 cell/pager

⚡ Indian railroad communications

Bart van Leeuwen <bart@ixori.demon.nl>

Fri, 9 Jun 2000 10:26:59 +0100 (BST)

The Dutch railways have been participating in a Dutch telecommunications company, and have been doing this for quite a few years already. It is very interesting to see this happen in India of course, but it is far from a new concept, and the pilot is likely aimed at local implications of this, and not at the technology as such.

Bart van Leeuwen bart@ixori.demon.nl - <http://www.ixori.demon.nl/>

⚡ Re: India piggybacking on railway controls (Bakowski, [RISKS-20.90](#))

"James Ryan \ (Private E-Mail\)" <james_ryan@attglobal.net>
Mon, 12 Jun 2000 14:03:25 +1200

Indeed, Japan Telecom did the same thing with Japan Railways capacity in the early 90s...

⚡ REVIEW: "Information Hiding Techniques for Steganography and

Rob Slade <rslade@sprint.ca>
Fri, 16 Jun 2000 08:09:20 -0800

Digital Watermarking

BKIHTSDW.RVW 20000504

"Information Hiding Techniques for Steganography and Digital Watermarking", Katzenbeisser/Petitcolas, 2000, 1-58053-035-4
%E Stefan Katzenbeisser
%E Fabien A. P. Petitcolas
%C 685 Canton St., Norwood, MA 02062
%D 2000
%G 1-58053-035-4
%I Artech House/Horizon
%O U\$69.00 800-225-9977 fax: 617-769-6334 artech@artech-house.com
%P 220 p.
%T "Information Hiding Techniques for Steganography and Digital Watermarking"

Steganography can be used for sending encrypted messages, but the primary emphasis in this volume is in the use of techniques for detecting forgery, theft of intellectual property, and modification of a digital object.

Digital watermarking is probably best known to the general public from the transparent logos used on cable channels to try and prevent, or at least identify, illegally taped copies of programs. Chapter one gives us a definition of steganography and digital watermarking, some history, and some editorial on the counterintuitive links between the technical partnership of encryption and digital signatures.

Part one outlines secret writing and steganography, the latter being the art of hiding a message in plain sight. Chapter two deals with the principles of steganography. Unfortunately, while the general principles are explained, the details require some number theory. The formal definitions that are used, for example, refer to axioms that are not presented in the text. Most of the techniques explained in chapter three are

graphical, but a few are applicable to text. Steganalysis is, of course, dependent upon the techniques being used, and various products are analyzed in chapter four.

Part two looks at watermarking and copyright. Chapter five examines watermarking principles and evaluation criteria. Techniques are described in chapter six. Chapter seven deals with the reasons that copyright marking technologies require highly robust algorithms and systems. Chapter eight reviews digital fingerprinting, for individual identification. Legal considerations are discussed in chapter nine, in regard to watermarking, the Internet, and copyright.

A common problem in many collective works is that the various submissions have differing styles and tend to overlap and repeat topics. While there are certainly stylistic differences between the chapters in this book, the authors/editors have kept repetition and duplication to a minimum.

copyright Robert M. Slade, 2000 BKIHTSDW.RVW 20000504
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

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

Call For Participation - RAID 2000

Herve Debar <deb@zurich.ibm.com>

Fri, 16 Jun 2000 16:31:16 +0200

Third International Workshop on the Recent Advances in Intrusion Detection

October 2-4, 2000, Toulouse, France, in conjunction with ESORICS 2000

This workshop, the third in an ongoing annual series, will bring together leading figures from academia, government, and industry to discuss state-of-the-art intrusion detection technologies and issues from the research and commercial perspectives.

RAID 2000 is being locally organized by ONERA in Toulouse, France, in conjunction with ESORICS 2000 (<http://www.cert.fr/esorics2000/>). The program committee invites submission of extended abstracts, to be made available on the RAID website.

Registration is available online at <http://www.raid-symposium.org/raid2000/registration.html>. A preliminary program is available at <http://www.raid-symposium.org/raid2000/program.html>.

[This is abridged for RISKS, but it did not mention that the advanced registration deadline is 16 Aug 2000. 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 20: Issue 93

Monday 3 July 2000

Contents

- [Collapse of UK air-traffic control computer](#)
[Ulf Lindqvist](#)
- [Sliced fiber-optic cable disrupts phone service in Northeast](#)
[Doneel Edelson](#)
- [State Department loses phone service](#)
[PGN](#)
- [Weld-done stake in phone lines](#)
[PGN](#)
- [Find security hole, get sued](#)
[Stanley Chow](#)
- [The low-down on the Berlin Fire Department Y2K-fiasco](#)
[Debora Weber-Wulff](#)
- [NATO creates computer virus that reveals its secrets](#)
[Monty Solomon](#)
- [Hacker endangers astronauts](#)
[Avi Rubin](#)
- [Burger King gives away CD-ROM with porn addresses](#)
[PGN](#)
- [Hotel phones that ID room occupants](#)
[Bertha](#)

- [Electronic signatures secure?](#)
[John P. Darrow](#)
[LucFrench](#)
 - [*The NYT* site exposes CIA agents](#)
[Monty Solomon](#)
 - [Re: UK Millennium Bridge instability](#)
[Tony Woolf](#)
[John Sullivan](#)
 - [Microsoft software *can* damage your hardware!](#)
[Rob Slade](#)
 - [Another Win95/DOS interaction](#)
[Jeremy Epstein](#)
 - [Y2K-leapyear hangover, human error or other tomfoolery?](#)
[Ari Ollikainen](#)
 - [Re: Network Solutions risks](#)
[Peter Sleggs](#)
 - [Personal train warning](#)
[Marc Salverson](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Collapse of UK air-traffic control computer

Ulf Lindqvist <ulf@csl.sri.com>

Sun, 18 Jun 2000 10:34:18 -0700 (PDT)

On 17 Jun 2000, thousands of would-be passengers were stranded when the main air-traffic control computer collapsed. The National Air Traffic Services computer was fixed later in the day, but the resulting congestion caused many people to spend the night at airports around the UK, and many flights were cancelled the next day as well. Heathrow and Gatwick were hardest hit, although other UK airports experienced severe delays. This was the second

time in a week that the computer system had failed. [PGN-ed,
from BBC,
Sunday, 18 June, 2000, 11:33 GMT
http://news.bbc.co.uk/hi/english/uk/newsid_796000/796018.stm]

Ulf Lindqvist, SRI International, 333 Ravenswood Ave, Menlo Park
CA 94025-3493
+1 650 859-2351, <ulf@sdl.sri.com> <http://www.sdl.sri.com/>

[Also noted by Dave Stringer-Calvert, Ursula Martin, Yves
Bellefeuille. PGN]

[I flew back from the East Coast on 25 Jun 2000, and
experienced
huge delays that were blamed alternatively on thunderstorms
and on
air-traffic control congestion. Airports in Boston, NY,
Philly, and
Washington were essentially shut down. PGN]

⚡ Sliced fiber-optic cable disrupts phone service in Northeast

"Doneel Edelson" <doneel.edelson@eulergroup.com>
Thu, 29 Jun 2000 12:38:12 -0400

Phone service in the Northeast was disrupted Wednesday evening
after a Bell
Atlantic fiber-optic cable was sliced in Lancaster PA, affecting
local
customers and callers from New York to Maryland using AT&T, MCI
WorldCom,
and other long-distance carriers routing through that area.
[PGN-ed from
CNN item and USA Today items, 28 Jun 2000]

⚡ State Department loses phone service

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

Mon, 21 Jun 2000 6:03:21 PDT

Heavy rains knocked out telephone service for two hours for the U.S. State

Department on the evening of 15 Jun 2000, and the backup batteries were

unusable because of an earlier fire. [PGN-ed

<http://www.cnn.com/2000/US/06/16/state.phonesout.ap/index.html>]

⚡ Weld-done stake in phone lines

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

Wed, 28 Jun 2000 7:19:12 PDT

In the last week of June 2000, during construction preparing for connecting the Bay Area Rapid Transit (BART) to the San Francisco Airport, a

droplet of welding material in a manhole just south of San Francisco caused

a fire that destroyed portions of 27 cables, wiping out telephone service to

25,000 customers; the process of replacing 800 feet of cable and correctly

reconnecting the many thousands of wires was expected to take at least two

weeks.

⚡ Find security hole, get sued

Stanley Chow <stanley.chow@cloakware.com>

Thu, 22 Jun 2000 09:59:04 -0400

A story in the local paper (*Ottawa Citizen*) reports that an Edmonton

man found a way to win at slot machines. The report is typically weak

with details; this is my understanding of what happened:

- WMS Gaming Inc. is the manufacturer of video slot machines
- there are back door easter-eggs on (some) blackjack machines that

give you a win.

- According to company lawyer, this has cost millions of dollars

- Mr. Yaghi (an independent software consultant) found it somehow

- Mr. Yaghi told the gaming commission and the company

- company sues him for ten million dollars, and got court order to

search his house

The parallels with the French smartcard episode are striking. I must

reluctantly come to the conclusion:

Crime pays a lot better than honesty.

Can anyone familiar with slot machines tell me how could this get through the QA process? Don't they do code-inspections?

Stanley Chow, Cloakware Corp, 260 Hearst way #311 Kanata,
Ontario K2L 3H1

Canada VP Engineering (613) 271-9446 x 223 stanley.
chow@cloakware.com

🔥 The low-down on the Berlin Fire Department Y2K-fiasco

Debora Weber-Wulff <weberwu@tfh-berlin.de>

Sun, 18 Jun 2000 19:22:21 +0200

The German computer biweekly magazine c't analysed the Y2K-fiasco that

caused the Berlin Fire Department to miss fires and lose fire trucks

this past New Year's Eve. See [RISKS-20.75](#) and [RISKS-20.82](#).

The major culprit was the security preparations themselves, it seems.

In order to avoid the Y2K problem, the programmers had decided to give 1999 13 months instead of the usual 12. Then, just before the New Year's, they installed a time server in order to prevent there being a problem when the system time of the computers was compared with the normal time which is broadcast in Germany on a special frequency. They missed one little thing: leading zeros. The operating system delivered dates as 1:12:99 while the time server used 01:12:99. But since the time server was not installed until after the 10th of December, it wasn't until midnight that the clock struck 13, or rather 1:13:99 instead of 01:13:99.

This caused another program to cough about a date discrepancy. So the people overseeing the systems tried to reboot the system [this at just past midnight on the first of January! -dww]. But it wouldn't reboot, because two of the computers were not configured properly. If they had ignored the error message, everything would have been okay!

Now, while the system was trying to reboot, the folks in the fire trucks got antsy. They didn't get acknowledgements for their reports of where they were. So they just pushed all the buttons, to see if the machine was dead. This flooded the system additionally with repeated status messages.

Finally, the network boards come into play. They had been named as the

culprits in the first round of finger-pointing. They had just been installed, and were misconfigured. They couldn't handle the traffic and began producing random errors. This confused the part of the system that keeps track of where the equipment currently is located, and then **it** died.

So they reverted to paper and pencil and fax. The fax machine which made up the major connection for the backup system needed 30 seconds per fax, but the reports were coming in faster than that, causing the fax cutter to jam. This meant that the reports were in the fax memory, but there was no way to get them out on paper, and a second fax machine was not available.

So thanks to c't for showing us that you can't be paranoid enough, you really need to keep all your equipment rebootable, and it might be a good idea to have a working back-up system. Luckily, the **other** guys got most of their Y2K-stuff right, so we didn't have Armageddon happening and didn't need to know where all the fire trucks were parked.....

Prof. Dr. Debora Weber-Wulff, TFH Berlin, FB Informatik,
Luxemburger Str. 10
13353 Berlin, Germany weberwu@tfh-berlin.de <http://www.tfh-berlin.de/~weberwu>

✶ NATO creates computer virus that reveals its secrets

Monty Solomon <monty@roscom.com>

Sat, 24 Jun 2000 12:31:38 -0400

Bungling NATO scientists have created a computer virus "by mistake", causing military secrets to find their way onto the internet. The virus, called Anti-Smyser 1, was created by scientists at NATO'S Kfor peacekeeping force headquarters in Pristina, Kosovo. They were seeking protection from virus attacks similar to those launched at NATO by the Serbs during the Kosovo conflict. But the experiment went wrong, and scientists accidentally unleashed the virus on themselves. The virus, which plucks documents from the hard drives of computers and sends invisible attachments to e-mails, recently resurfaced at the Czech ministry of defence.
<http://www.the-times.co.uk/news/pages/sti/2000/06/18/stinwenws01024.html>

Hacker endangers astronauts

Avi Rubin <rubin@research.att.com>

Mon, 3 Jul 2000 01:26:04 GMT

According to the BBC, 3 Jul 2000, a computer hacker endangered shuttle astronauts in 1997 by overloading NASA's communication system after tapping into the NASA system monitoring the astronauts' on-board medical signs while docking with Mir. Apparently, NASA has experienced more than 500,000 cyber attacks in the past year. [PGN-ed]

Burger King gives away CD-ROM with porn addresses

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

Mon, 26 Jun 2000 5:18:53 PDT

Declan McCullagh's news distribution included an item from Paul McMasters

written by Jonathen Lambeth that Burger King distributed free with

children's meals a CD-ROM including the Net Nanny filtering program that

with a few extra mouse clicks gets you a list of more than 2000 Internet

porn sites. [PGN-ed]

✶ Hotel phones that ID room occupants

That Funky Chick <bertha@mhn.org>

Sun, 18 Jun 2000 21:18:49 GMT

This weekend some relatives and I were staying at a fairly nice hotel. At

one point two of us were in the lounge, and I called the room to let my

mother know where we were in case she wanted to join us. When I dialed

our room number, my mother's name (the name the room was reserved under)

showed up on the phone's LCD.

I'm sure there are very good reasons why this would be a desirable thing.

Certainly it would have been immediately clear to me if I had accidentally

misdialed and called someone else's room. However, I can also think of

some instances when this feature might not be welcome. For example,

someone interested in fraud could conceivably call a room number at random,

then use that occupant's name and room number to sign his guest check at the hotel restaurant. No picture ID is required during this process; the real occupant wouldn't be aware of fraudulent charges until his final bill was presented at checkout.

For another example, a child who is ordinarily old enough to be left alone in a safe hotel room might not be discriminating enough to be suspicious if a stranger at the door knows a parent's name. Parents can warn their pre-teen not to open the door for "room service," but would probably not think to warn the child not to believe someone claiming to be sent by "Your mommy, Jane Smith."

I don't doubt that RISKS readers will be able to come up with other scenarios.

-Bertha

⚡ Electronic signatures secure?

<john.p.darrow@wheaton.edu>

Fri, 30 Jun 2000 15:34:13 -0400 (EDT)

Message: Note Clinton's rather poor password.

President Clinton on Friday used an electronic card and his dog's name as a password to "e-sign" into law a bill that makes electronic signatures as valid as their ink counterparts. [...] "Now, let's see if this works," the self-proclaimed technologically challenged Clinton said with

a chuckle
as he inserted the smart card into the computer and punched in
his dog's
name, Buddy, as the password.

[See <http://www.pfir.org> for a position paper on this
legislation. PGN]

⚡ **Electronic signatures secure?**

<LucFrench@aol.com>

Fri, 30 Jun 2000 16:02:22 EDT

The RISK here should be obvious. No, not the bill itself (that's
a subtle
RISK), but using your dog's name as a password, and announcing
the fact via
an international news service.

⚡ ***The NYT* site exposes CIA agents**

Monty Solomon <monty@roscom.com>

Sat, 24 Jun 2000 12:00:33 -0400

A freedom of information activist plans to publish online a
classified CIA
document that was pulled from *The New York Times'* site after
newspaper
officials learned it exposed the identities of Iranians involved
in the 1953
U.S. and British-backed coup that overthrew Iran's elected
officials. *The
Times* used the graphic to accompany an article detailing the
coup. In a
technical glitch, those who visited the Times website on June 16
were able

to read the names of the agents when they downloaded the graphic. *The Times* put a layer of black boxes over the names in the 200-page Portable Document Format file, allowing viewers who "froze" the page while it was being downloaded to read the names underneath. [Wired News Report, 23 Jun 2000, <http://www.wired.com/news/politics/0,1283,37205,00.html>]

✈ Re: UK Millennium Bridge instability ([RISKS-20.92](#))

"Tony Woolf" <mail@tonywoolf.co.uk>
Tue, 20 Jun 2000 18:02:24 +0100

London's much publicised pedestrian Millennium Bridge over the Thames closed the day after it opened because it swayed alarmingly when large crowds crossed it. The public had been assured that the design, which is novel, had been extensively tested by Ove Arup using computer simulations and scale models.

New Scientist magazine (17 June 2000) quotes John Dickens, a civil engineer at Loughborough University UK: "Even the most sophisticated simulation programs have assumptions built into them and until you build the whole thing you've still got a degree of uncertainty".

The risk: pushing a simulation program to deal with a novel design. I wonder whether those using the program had a clear idea of exactly what assumptions were built into the program. Very likely no-one knows what most

of the assumptions are because many of them probably arise out of theories that work in the usual cases.

More generally, any novel design is likely to show up false assumptions in the usual design processes, whether or not those assumptions reside in a computer program. Therefore extra cost and time should be allowed specifically for the novelty factor, quite apart from that allowed for the known technical difficulties.

Tony Woolf

🚩 Re: UK Millennium Bridge instability ([RISKS-20.92](#))

John Sullivan <john@kanargh.force9.co.uk>

Sat, 17 Jun 2000 16:38:17 +0100

On Friday 16 June 2000 you wrote:

> Anything there on computer modeling?

The Ove Arup homepage has a section on the engineering of the bridge at:

<http://www.arup.com/MillenniumBridge/>

Not too much detail, but plenty of pretty pictures. Quotes:

> Extensive analysis and wind tunnel testing have been carried out to

> ensure the bridge is stable in a one in 10,000 year gale.

> Analysis has been made of the motions resulting from pedestrians moving

> across the bridge to keep them within acceptable levels.

These were

> tested on a shake table by the design team at Southampton

University.

> The pier response above ground to load was determined from
computer
> modeling.

> We found that the maximum possible impact force from a ship
bow from the
> boats traveling on the Thames on the pier is in the order of
35MN -
> equivalent to 26 000 people pushing at once. The bridge piers
will move
> just 160mm sideways under this force, and continue to support
the bridge.

150,000 people crossed on the first day. I'll take a wild stab
and
estimate that that means about 500-2000 people on the bridge at a
time, on average. (Given the size of the bridge as 320x4m, this
is
reasonable. You could probably comfortably fit 2500 walking
people on
at a time.) Under that load it was moving 8" (200mm).

<http://www.arup.com/MillenniumBridge/images/videos/stat.gif>

models the
cable stresses up to a load of 5000 people. (5000 is the maximum
standing load.)

Overall they seem do have done a range of computer and physical
modeling including a second independent computer modeling team,
but
vastly underestimated the number of people it would have to
reliably
support. Assuming the models were correct (and as they say, the
stresses involved make this a ground-breaking project) you're
still
not going to get good outputs if your inputs are an order of
magnitude
out.

John

⚡ Microsoft software *can* damage your hardware!

Rob Slade <rslade@sprint.ca>

Fri, 30 Jun 2000 08:47:22 -0800

Remember the good old days? High speed disk drives, heavy aluminum platters that sometimes fractured, at speed, sending pieces of metal out through the sides of the drive?

Yesterday one of my students brought in a picture he had scanned of a bunch of fragments of CD-ROM. He had been installing Microsoft LinksGolf 2000. While disk 2 (of 3) was in the drive, there was a sudden noise, the drive bay popped open, and out flew various pieces of plastic. These were moving fast enough that one cut him on the back. A number of smaller pieces are obviously still in the machine: he got the bay closed, but now it won't open any more.

This drive is (or, at least, used to be) a 52x drive, so clearly we are getting up there in speed.

The risks, in terms of hardware damage, software loss, and personal injury, are plain, but some interesting questions remain.

Are we reaching the limits of safe operation with plastic disks? Or is it only defects in manufacture that cause this type of problem?

Does the use of Microsoft LinksGolf void the warranty on the drive?

Who do you sue for personal pain and suffering, the drive

manufacturer, or
Microsoft?

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

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

⚡ Another Win95/DOS interaction

Epstein Family <jepstein@monumental.com>

Sat, 17 Jun 2000 22:11:09 -0400

Several years ago there was a series of postings in RISKS about the unexpected interactions between Win95 and the underlying DOS operating system.

I just discovered another one. I run Win95 at home (works just fine on my 133MHz Pentium). I wanted a list of all the files in a directory, so I could print it. Of course there's no easy way to do this directly from the Windows Explorer, so I started a DOS window, typed "dir /on >foo.txt" (where "/on" means "sort in alphabetic order"), and printed the resulting file. Unfortunately, "/on" *really* means "sort in alphabetic order by the 8.3 short name of the file". There doesn't seem to be a way to tell the "dir" command I want it to sort the real name of the file, not the abbreviation.

Luckily I have a handy UNIX system with a decent set of tools so I can turn the list into what I really want...

The RISK is assuming that software does what it's documentation says it does.

--Jeremy

⚡ Y2K-leapyear hangover, human error or other tomfoolery?

Ari Ollikainen <Ari@OLTECO.com>

Fri, 30 Jun 2000 19:23:20 -0700

Today my CDMA GTE wireless cellphone is displaying the date as 6/31/00...which, as everyone knows, doesn't exist!

Anyone from GTE wireless willing to provide an explanation?

Ari Ollikainen, OLTECO, P.O. BOX 3688, Stanford, CA 94309-3688
Networking Architecture and Technology Ari@OLTECO.com 1-415.517.3519

⚡ Re: Network Solutions risks (Rhodes, [RISKS-20.92](#))

Peter Sleggs <peters@belsys.com>

Sun, 18 Jun 2000 08:53:54 -0500

It is not difficult to NOT receive the invoices, I have 2 domains I pay for - Domain 1 usually goes smoothly, but last year domain 2 did NOT result in ANY paper invoices - required to get payment generated via the accounting process, I had to bring this to Network Solutions attention and was told - just pay it via credit card

- Without an invoice this comes out of MY pocket
- No invoice results in hassles with auditors

- The invoice they generate does not include the Canadian GST [goods & services tax] which they are required to collect if they provide services to Canada [at least the bean counter says so]
- With not collecting the taxes the risk is taking on the Canadian tax man :) [which in my opinion would be a nice thing to happen to NS]

This year's screwup - I decided to pay the domain 1 for multiple years and take advantage of the discount offered ... two weeks after I did this I got a "Deactivation notice", the web interface did NOT pay the invoice and said it did, BUT once again they do not close the loop and provide a tracking number like the phone payment interface does, so the attempt to deal with billing@networksolutions.com starts again.

Domain 2 is also missing the paper invoice this year :(

So the non-payment of the fees may simply be another case of NS not properly sending out bills, with all the obvious risks there.

⚡ Personal train warning

Marc Salverson <marc@undergraph.com>

Fri, 23 Jun 2000 08:33:03 -0500

On 22 Jun 2000, Paul Harvey reported that most people who have died at railroad crossings "didn't hear the train coming". He must have some inside information.

The point to the story was that someone is marketing a device to

be
installed in a car that will alert the occupants that a train is
coming. Do
you think they claim that's the only time it could possibly
alert? No risk
here!

That might be more tempting to hack than a tornado siren.

Marc <marc@undergraph.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 20: Issue 94

Friday 7 July 2000

Contents

- [Software upgrade cancels hundreds of train tickets](#)
[Ian Shorrocks](#)
- [Lottery coincidence reported by Infobeat caused by computer crash](#)
[Bob Heuman](#)
- [Total power outage at Sydney Airport leaves 20 planes circling](#)
[Mike Hogsett](#)
- [U.K. ATC System Failure](#)
[Andres Zellweger](#)
- [Re: Collapse of UK air-traffic control computer](#)
[Mark Richards](#)
- [Mix-up sends Spanish bank e-mail to Virginia BBoard](#)
[NewsScan](#)
- [17,000 bank details plucked from GST Site](#)
[Keith A Rhodes](#)
- [One more Y2K glitch, on countdown](#)
[Floyd Johnson](#)
- [Australian DST rules changed for Olympics](#)
[Mark Lutton](#)
- [Cyber-extortion](#)
[Doneel Edelson](#)

- [Hacker did *NOT* endanger shuttle astronauts](#)
[Jay D. Dyson](#)
 - [Norton Antivirus 2000 defect on Win2000 Content](#)
[Jeremy Epstein](#)
 - [Re: Microsoft software *can* damage your hardware!](#)
[Peter Van Eynde](#)
 - [REVIEW: "Firewalls: A Complete Guide", Marcus Goncalves](#)
[Rob Slade](#)
 - [CERIAS symposium](#)
[Gene Spafford](#)
 - [The Software Engineering Symposium](#)
[Carol Biesecker](#)
 - [Call for registration ESORICS and RAID 2000](#)
[Frederic Cuppens](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Software upgrade cancels hundreds of train tickets

Ian Shorrocks <IanShorrocks@compuserve.com>

Thu, 6 Jul 2000 14:49:40 -0400

Guildford Station in Surrey, UK is one of many stations fitted with much hated automatic ticket barriers by the operators, South West Trains Ltd. The barrier checks the magnetic stripe on the back of the ticket to determine if the ticket is valid and admits you to the station platforms or allows you to leave.

As far as anyone is aware, there was nothing wrong with the barriers other than the annoyance they cause as queues form during the Rush hours, as the gates open and close somewhat slowly.

Last week, CTS, the company that provided the barriers, decided

to upgrade
the software. Long suffering Risks Digest readers will not be
surprised to
learn that the operation of the barriers following the upgrade
was not as
CTS; the Rail company or anyone else expected. Instead of
allowing the
holder of a valid ticket access to the platforms, the barrier
instead
erased the information on the magnetic stripe, thus permanently
invalidating the ticket. South West Trains then had the problem
of
reissuing all the affected tickets (several hundred by all
accounts) and
manually checking tickets until the problem was resolved.

There is no substitute for complete lack of proper testing or for
un-necessary software changes.

The risk is: does the same cavalier attitude to testing apply to
the
software running the signalling system?

✶ Lottery coincidence reported by Infobeat caused by computer crash

<rsh@idirect.com>

Tue, 04 Jul 2000 00:14:42 -0400

Oregon Lottery officials thought it was a joke when someone
called to say
The Columbian had published the winning Pick 4 lotto numbers a
few hours
before they were drawn. When they learned the caller was right,
they
dispatched Lloyd W. Beil, a detective with the Oregon State
Police gaming
enforcement section. "Game security is our most valuable
commodity," said

David Hooper, an Oregon Lottery spokesman. As it turned out, the newspaper's computer system in this city across the Columbia River from Portland, Ore., crashed Wednesday. In the scramble to re-create a lost page, a copy editor mistakenly pulled the winning Pick 4 numbers from Virginia and billed them as the Tuesday night's winning pick in Oregon. Those same winning numbers, 6-8-5-5, were also drawn later Wednesday evening in Oregon. [AP item, Lottery numbers published by fluke (*Infobeat*, Jul 3 2000) <http://www.infobeat.com/stories/cgi/story.cgi?id=2567832665-960>

R.S. (Bob) Heuman, Toronto, ON, Canada <bob.heuman@intria.com><rsh@idirect.com>

⚡ Total power outage at Sydney Airport leaves 20 planes circling

Mike Hogsett <hogsett@csl.sri.com>
Fri, 07 Jul 2000 14:19:10 -0700

Another story of primary and secondary power system failure...

[On the evening of 6 Jul 2000, the main power and the backup power for the Sydney air-traffic control system both failed at 6 p. m., a period of peak activity. The power outage lasted for about two minutes, and it took another 10 minutes to reboot the computers.

The fallback strategy involved "pilot-to-pilot communications and predetermined holding patterns." The Community and Public Sector

Union national organizer Alistair Waters was quoted: ``As you keep

cutting back and cutting back, the chances of failure happening grow and grow. And that does risk safety.' ' PGN-ed]

http://dailynews.yahoo.com/h/nm/20000707/od/airport_dc_1.html

✶ U.K. ATC System Failure

Andres Zellweger <ZellwegA@cts.db.erau.edu>

Thu, 6 Jul 2000 08:42:42 -0400

According to **Aviation Week**, 26 Jun 2000, the U.K. ATC computer failure reported in [RISKS-20.93](#) was due to Flight Processing Software at the West Drayton ATC Center. As a result of the failure, flight progress strips "had to be produced manually, a labor-intensive practice that forced NATS to slow down the amount of traffic in the U.K. airspace. NATS eventually reinstated the previous software program, which stabilized the system." The new software was developed internally by NATS and had been installed three weeks prior to the failure.

It is interesting to note that, while the system recovered after four hours, the effects of the failure was felt for the entire weekend and as far away as Paris and Frankfurt. (I sat on the ground at Malpensa on a flight bound to IAD for at least two hours waiting to be rerouted to avoid the U.K. airspace.)

The other problem with the U.K. ATC system reported in [RISKS-20.93](#) occurred on 9 Jun 2000. It was also a problem with the flight data

processing
software. That 20-minute failure was due to human error --
repeated "bad"
flight data input from another ATC Center. The problem was
fixed through
procedural means.

✈ Re: Collapse of UK air-traffic control computer

"Mark Richards" <mark.richards@massmicro.com>

Thu, 6 Jul 2000 09:45:19 -0400

PGN noted that huge delays in US Domestic air service were
"blamed
alternatively on thunderstorms and on air-traffic control
congestion",
noting Boston's ugly, congested, dirty, confusing, unfriendly
Logan airport
among them (sorry, couldn't help myself).

Add another reason: it's reported locally that pilots from many
airlines are
refusing landing clearances that involve the simultaneous use of
a crossing
active runway for departure. A recent incident where takeoff
clearance was
given to one flight while another was landing is used as case-in-
point: they
nearly collided (reports were from 100-300 feet vertical
separation) at the
intersection! The old saying "Arrive Alive" certainly fits.

Mark Richards <mark.richards@massmicro.com>

✈ Mix-up sends Spanish bank e-mail to Virginia BBoard

"NewsScan" <newsscan@newsscan.com>

Fri, 07 Jul 2000 07:09:51 -0700

One of Spain's largest banks -- and its most aggressive in terms of moving operations onto the Internet -- is suffering from an identity crisis that has resulted in thousands of messages being routed to Bulletin Board VA, run by a rural Virginia man who publishes a weekly shopper with a circulation of 10,000. Banco Bilboa Vizcaya Argentaria, which goes by the acronym BBVA after Banco Bilbao Vizcaya merged with Argentaria SA last fall, is the owner of the "grupobbva.com" domain name, but many employees, customers and outside vendors mistakenly send their sometimes-sensitive e-mail to "bbva.com," a domain name owned by Bulletin Board VA. "When all this e-mail started coming in, I didn't know who to contact. I didn't know who to talk to," says Bulletin Board VA owner Jim Caldwell. "To me it is beyond the stage of funny." Some of the messages contain bank account numbers and balances, and at least one contained confidential information about a possible bank acquisition. BBVA says it's in the process of changing its domain name to "bbva.es," and hopes that will solve the problem. Caldwell certainly hopes so -- he says he spends up to two hours a day clearing his server of the mislabeled messages. [*Wall Street Journal*, 7 Jul 2000 <http://interactive.wsj.com/articles/SB962887042191508928.htm>; NewsScan Daily, 7 Jul 2000]

⚡ 17,000 bank details plucked from GST Site

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

Thu, 29 Jun 2000 10:35:15 -0400

In Australia, someone claimed to have accessed a Treasury Department Web site www.gstassist.gov.au that had essentially no security. By indexing from 1 to 17,000, he was able to obtain the bank records of that many registered GST Startup certificate suppliers. (There were apparently 27,000 records in all, but access stopped when the site was disabled.) He then sent e-mail to each these companies (which can honour a \$200 GST-related rebate on computers, software, services and other items required for small and medium companies to prepare for Australia's new taxation system) with its own relevant details. [Source: Bank details plucked from GST Site, By Nicole Manktelow, ZDNet Australia, and Paul Zucker, PC Week Australia; PGN-ed]

⚡ One more Y2K glitch, on countdown

Floyd Johnson <floydj@netins.net>

Fri, 07 Jul 2000 12:43:50 -0400

The U.S. Naval Observatory in Washington, DC, has a web site that lists a count down timer to "Countdown to the Year 2000 !":

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

and when the link is followed we do find the "USNO Millennium Program".

However, and here is the kicker, the millennium counter is not counting down

to 2000, but to 2001. The pages cite 1 Jan 2001 as the beginning of the new

millennium:

<http://psyche.usno.navy.mil/millennium/>

Golleeeee ... if the US Navy can't get it right, how can the rest of us

expect to get there on time [:)]. [Both pages are written by the USNO.]

Floyd H. Johnson, 87 Parkway Drive, North Chili, NY 14514
1-716-594-0942 floydj@netins.net

[On the other hand, there is an explanation on the latter site that the next millennium begins on 1 Jan 2001. Go figure. I presume it is last year's program recycled. PGN]

⚡ Australian DST rules changed for Olympics

"Mark Lutton" <Mark.Lutton@newsedge.com>

Thu, 6 Jul 2000 17:48:23 -0400

Several Australian states have changed the Daylight Savings Time rules so

that DST will be in effect for the year 2000 Olympic Games in Sydney in

September. (late winter for them). Normally DST begins in October.

I suppose the benefits are substantial. Quite a bit of electricity for stadium lighting will be saved.

I wonder if anyone considered the costs and the risks. This

affects just about every computer in Australia, and many automated installations like radio stations, time-lock bank vaults and security systems. Microsoft is taking it calmly and has issued a notice at <http://www.microsoft.com/australia/support/timezone/2000.htm>.

I guess there was some reason they couldn't just schedule every event to start an hour earlier.

⚡ Cyber-extortion

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

Thu, 6 Jul 2000 10:31:29 -0400

Instances of "cyber-extortion" are increasing dramatically, according to Dave Marziliano, an FBI agent in New York who specializes in computer crime and security. Cyber-extortion involves hackers blackmailing companies by threatening to turn over purloined strategic data to their competitors. Marziliano says these cases are growing due to an increase in the number of hackers, particularly in underdeveloped countries. Most incidents involve relatively small amounts of money, \$50,000 to \$100,000, which many companies would rather pay than take the chance of losing competitive advantage.

[Source: InformationWeek Online, columnist John Soat, and InformationWeek magazine, July 3, 2000, page 150.]

⚡ Hacker did *NOT* endanger shuttle astronauts (Re: Rubin, [RISKS-20.93](#))

"Jay D. Dyson" <jdyson@techreports.jpl.nasa.gov>
Wed, 5 Jul 2000 13:56:26 -0700 (PDT)

Bob Jacobs/Dwayne Brown
Headquarters, Washington, DC
(Phone: 202/358-1600)

July 3, 2000

Ed Champion/Eileen Hawley
Johnson Space Center, Houston, TX
(Phone: 281/483-5111)

COMPUTER HACKER NEVER ENDANGERED SHUTTLE ASTRONAUTS

News reports that a computer hacker endangered the lives of Space Shuttle astronauts during a 1997 mission are wrong. A report from the British Broadcasting Corporation (BBC) said a hacker compromised NASA computers, endangering the lives of American astronauts.

NASA's Inspector General's office found that during the STS-86 mission in September of 1997, the transmission of routine medical information was slightly delayed due to a computer hacker. However, the transmission was successfully completed.

At no time was communication between NASA and the astronauts compromised. The communication interruption occurred between internal ground-based computer systems.

There has never been an interruption of communication service with the Shuttle due to computer hacker attacks. The command and control communications links between Mission Control and a Space Shuttle

in orbit
are extremely well insulated.

The 1997 incident is currently under investigation by NASA
Inspector
General's office.

Courtesy of NASA HQ. Send questions to them, not me.

Side note: Knowing what I know about how the mission-critical
systems are

not on the Net, the BBC story rings utterly false. JDD
[Jay, I guess you might be SURPRISED on your supposition! PGN]

⚡ Norton Antivirus 2000 defect on Win2000 Content

"Jeremy Epstein" <jepstein@webmethods.com>

Thu, 6 Jul 2000 16:53:27 -0400

Seems that if you're one of those vigilant people who always
download the
latest virus definitions, you could be in trouble. If you
downloaded Norton
Antivirus 2000's virus definitions between June 16 and 19 and
then used them
on Windows 2000, you would hang the system.

The problem stems (in part) from the fact that they appear to be
downloading
some sort of active content ("new script file scanning
techniques" is the
way they described it), and those got confused by certain device
files.

Security software shouldn't (a) dynamically load updates to
itself or (b)
reduce reliability!

⚡ Re: Microsoft software *can* damage your hardware! (Slade RISK-20.93)

Peter Van Eynde <pvaneynd@debian.org>

Wed, 5 Jul 2000 23:31:56 +0200

> Are we reaching the limits of safe operation with plastic
disks? Or is it
> only defects in manufacture that cause this type of problem?

The German magazine C'T did a report on a similar case a few months ago. Their conclusion was that a hairline fracture in the plastic ring that surrounds the center hole can cause the CD to break-up under the stress of a X-speed CD-ROM drive.

They advised to check your CD's for hairline fractures or/and to use software to artificially slow down the CD drive to a more reasonable speed. This also has the nice side-effect of reducing the whine...

⚡ REVIEW: "Firewalls: A Complete Guide", Marcus Goncalves

Rob Slade <rslade@sprint.ca>

Wed, 5 Jul 2000 08:00:32 -0800

BKFWCMGD.RVW 20000517

"Firewalls: A Complete Guide", Marcus Goncalves, 2000, 0-07-135639-8,
U\$54.95

%A Marcus Goncalves goncalves@process.com goncalves@arcweb.com
%C 300 Water Street, Whitby, Ontario L1N 9B6

%D 2000
%G 0-07-135639-8
%I McGraw-Hill Ryerson/Osborne
%O U\$54.95 800-565-5758 fax: 905-430-5020
%P 678 p. + CD-ROM
%T "Firewalls: A Complete Guide"

Despite the change of name, this is not just essentially the second edition of "Firewalls Complete" (cf. BKFWCMP.L.RVW), it is identical, right down to the price. While there is a large amount of information in this book, and a particularly valuable compilation of vendor data, I am not sure that I can agree with the claim to be complete, even though the preface says it has been expanded. (The only specific expansion mentioned involves protocols.) It is difficult to point out particular gaps in the work, since the whole volume could still use a thorough reorganization.

Part one has been renamed to reflect the emphasis on TCP/IP. Chapter one deals with the TCP/IP suite of protocols. It does address protocol related weaknesses, but the protocols and attacks are not related, appearing in disorganized and even random material. Some attacks are described incorrectly, and sections even seem to contradict each other, such as the text emphasizing login controls and then discussing IP spoofing, which takes over legitimate logins. This appears to set the stage for a technical treatment of the subject. Networking details continue in chapter two with an overview of the various connection methods over the net. I am always delighted to get more information about new Kermit products, but I would

sympathize with any reader who was confused about what this material may have to do with firewalls. Encryption gets a brief review in chapter three. The content gets the basics across, but is of uneven depth between topics. Chapter four does start to provide security, and specifically firewall, related information in regard to the Web, but also includes a ten page CGI script that might be less useful. The data is good, but seems to be somewhat random and unstructured. Advanced Web security areas (including a more detailed examination of ActiveX vulnerabilities) is found in chapter five. Chapter six looks at much the same material.

Firewall technologies, implementations, and limitations are discussed in part two. Chapter seven attempts to define firewalls and describe firewall technologies. The discussion of firewall types has been expanded, but is still confused. The chapter also suffers from duplicate sentences and even paragraphs, and obviously could have used another copy edit. Vulnerabilities of individual Internet applications are the subject of chapter eight, but many concerns mentioned are more potential than actual (and thus difficult to defend against) while a good deal of the content (including yet another complete, ten page Perl script, this one a version from three years before the first) is repeated from earlier chapters. "Setting Up a Firewall Security Policy," in chapter nine, is much broader, touching on many security topics that may have little or nothing to do with firewalls. An example is the information on viruses, which is generally

trite. The overview of antiviral software betrays no knowledge of activity monitoring or change detection classes of programs. The recommended protection procedure suggests copying downloaded programs to a floppy disk rather than the hard disk, which is both useless (malicious software invoked from floppy will generally happily destroy data on your hard drive) as well as being impractical in these days of enormous packages. The more effective approach would involve a type of firewall: an isolated machine that could download software and test it before the programs were used on production machines. Chapter ten is supposed to address issues of design and implementation, but deals primarily with considerations for evaluation of specific products, as well as some suggestions for what to do once you've been hit. The question of design is made more problematic by the fact that the second major type of firewall Goncalves proposes, an application gateway, while first mentioned in chapter seven, is not defined until chapter eleven as a more generic form of a proxy server, which is itself first mentioned in chapter five but not described until this point. Chapter twelve covers basic auditing of the firewall, while chapter thirteen mentions a few firewall products.

Part three is chapter fourteen, which lists firewall vendors and products.

Descriptions of the products are extensive, and sometimes technically detailed, but it is difficult to call them evaluations, since there is little analysis of strengths and weaknesses. It is also hard to

make

comparisons, since there is little similarity of format in the entries.

Appendix A is a collection of vendor contact information.

Goncalves' writing on any given section is quite readable.

Explanations are

clear and illustrations can even be amusing. At times it seemed that the

material was moving into common traps and misconceptions, but ultimately the

analysis is generally balanced and realistic. However, in some cases there

is an apparent contradiction between one paragraph and the next. The

incongruity disappears on more rigorous scrutiny, but the text can be

startling. In addition, the structure of the book, both overall and within

individual chapters, leaves something to be desired. It can be difficult to

follow developing concepts, and also to use the book as a reference by going

back to specific topics to pick up particular points.

As an adjunct to Cheswick and Bellovin's "Firewalls and Internet Security"

(cf. BKFRINSC.RVW) or Chapman and Zwicky's more practical "Building Internet

Firewalls" (cf. BKBUINFI.RVW), this work does have useful information. As a

reference or introduction it falls short.

copyright Robert M. Slade, 1998, 2000 BKFVCMGD.RVW 20000517

rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca

pl@canada.com

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

 **CERIAS symposium**

Gene Spafford <spaf@cerias.purdue.edu>

Sat, 24 Jun 2000 20:42:15 -0500

CERIAS (Center for Education and Research in Information Assurance and Security) will be co-sponsoring a symposium on requirements engineering for information security and privacy. From the announcement: Security requirements for new electronic commerce and Internet applications exceed the traditional requirements for network security and traditional software systems. Security requirements are more complex and increasingly critical. Informally stated and de facto requirements are often of critical importance in the design and operation of these systems, but they are frequently not taken into account.

The symposium is intended to provide researchers and practitioners from various disciplines with a highly interactive forum to discuss security and privacy-related requirements. Specifically, we encourage those in the fields of requirements engineering, software engineering, information systems, information and network security as well as trusted systems to present their approaches to analyzing, specifying and testing requirements to increase the level of security provided to users interacting with pervasive commerce, research and government systems.

We intend this to be a significant event in developing new approaches to better security design and operation. We would like to ask your help to ensure that this happens.

Please let colleagues and other likely-interested parties know about this symposium. You can print off copies of the CFP <<http://www.cerias.purdue.edu/homes/spaf/cfpSREIS.pdf>> and circulate them. You can also point people to the symposium WWW page: <<http://www.cerias.purdue.edu/SREIS.html>>.

You can also think about submitting something to be considered!

✶ The Software Engineering Symposium

Carol Biesecker <cb@sei.cmu.edu>

6 Jul 2000 15:58:18 GMT

impacts 2000 - The Software Engineering Symposium
18-21 September 2000
Grand Hyatt at Washington Center, Washington D.C.

The most up-to-date information, including the Preliminary Program, Housing, Local, and Registration details, can be found on our Web site at
<http://www.sei.cmu.edu/products/events/symp/>

The Software Engineering Institute (SEI) Software Engineering Symposium provides a forum for discussing high-payoff emerging practices that software organizations can use today. Symposium sessions will describe current activities and research in the SEI technical program of work. These SEI efforts produce results that enable members of the software community to deliver software-intensive systems predictably better, faster, and cheaper.

By July 19, 2000, to express your interest, contact

Software Engineering Institute
Symposium Conference Coordinator
Carnegie Mellon University
Pittsburgh, PA 15213-3890
Phone: 412 / 268-3007
FAX: 412 / 268-5556
E-mail: symposium@sei.cmu.edu

For more information about the Symposium, contact
Symposium 2000 Conference Coordinator
Phone: 412 / 268-3007
FAX: 412 / 268-5556
E-mail: symposium@sei.cmu.edu

For general information about the SEI or to be added to our
mailing list,

SEI Customer Relations
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
Phone: 412 / 268-5800
FAX: 412 / 268-5758
E-mail: customer-relations@sei.cmu.edu

Call for registration ESORICS and RAID 2000

Frederic Cuppens <Frederic.Cuppens@cert.fr>
Tue, 27 Jun 2000 19:25:09 +0200 (MET DST)

ESORICS 2000 Preliminary programme and call for Posters
6th European Symposium on Research in Computer Security
October 4-6, 2000, Toulouse, France
<http://www.cert.fr/esorics2000/>

Organised by ONERA Centre de Toulouse
with CNAMTS-CESSI and LAAS-CNRS.

Registration form is available at
<http://www.cert.fr/esorics2000/register.html>

ESORICS 2000 is jointly organized with RAID 2000:
3rd International Workshop on the Recent Advances in
Intrusion Detection

October 2-4, 2000, Toulouse, France

<http://www.raid-symposium.org/raid2000/>

⚡ Safecomp 2000 - Programme + Registration

safecomp2000 <safecomp2000@tbm.tudelft.nl>

Tue, 4 Jul 2000 08:33:52 +0200

Sender: "Koornneef, Floor" <f.koornneef@tbm.tudelft.nl>

SAFECOMP 2000 - Programme & Registration

19th International Conference on
Computer Safety, Reliability and Security

October 24-27, 2000

ROTTERDAM, The Netherlands

The provisional programme of the Safecomp 2000 event and
registration

information are now available:

<http://www.wtm.tudelft.nl/vk/safecomp2000>

Safecomp 25-26 Oct will review the state of the art, experiences
and new

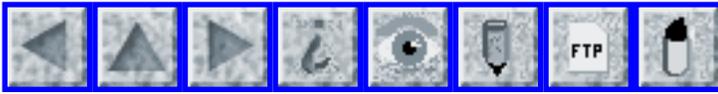
trends in the areas of computer safety, reliability and security
regarding

dependable applications of computer systems. There are also
five half-day

tutorials 24 Oct and 27 Oct. MORE INFORMATION:

<http://www.wtm.tudelft.nl/vk/safecomp2000>

E-mail: safecomp2000@wtm.tudelft.nl



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 95

Wednesday 19 July 2000

Contents

- [Anti-spam legislation](#)
[NewsScan](#)
- [Google allows anonymous spam](#)
[Lloyd Wood](#)
- [British law would allow police to intercept e-mail](#)
[NewsScan](#)
- [Clinton administration plans on wire taps & encryption](#)
[NewsScan](#)
- [ID theft finally coming to the fore](#)
[PGN](#)
- [Mother's maiden name as security check](#)
[Bill Tolle](#)
- [Navy to use Windows 2000 on aircraft carriers](#)
[Nancy Leveson](#)
- [House rejects Internet gambling bill](#)
[NewsScan](#)
- [Italian crash exposes risks of online stock trading](#)
[Keith A Rhodes](#)
- [DC Metro can't label rerouted trains](#)
[Wm. Randolph Franklin](#)

- [Illinois man dies after utility cuts power](#)
[Bill Higgins](#)
 - [Fox network misprograms time on US VCRs for a year](#)
[Michael D. Crawford](#)
 - [Company lost domain name](#)
[Arthur J. Byrnes](#)
 - [Royal Mail claims web orders encrypted when they aren't](#)
[Gary Barnes](#)
 - [London Underground magnetic ticket bug](#)
[Boyd Roberts](#)
 - [Man charged with breaking into NASA computers](#)
[Keith A Rhodes](#)
 - [A self-referential risky accident](#)
[Michael L. Cook](#)
 - [Re: Australian DST rules changed for Olympics](#)
[Fraser McHarg](#)
 - [Re: Software upgrade cancels train tickets](#)
[Matt Fichtenbaum](#)
 - [Re: UK Millennium Bridge instability](#)
[Charles Arthur](#)
 - [Re: Another Win95/DOS interaction](#)
[Lloyd Wood](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Anti-spam legislation

"NewsScan" <newsscan@newsscan.com>

Wed, 19 Jul 2000 12:28:55 -0700

The U.S. House of Representatives passed 427-1 a bill that would require senders of unsolicited commercial e-mail messages to provide a valid return e-mail address that recipients of the messages could use to take them off the mailing list. Under the law, the Federal Trade Commission

could bring
legal actions against spammers who willfully ignore it. Violators
could also
be sued by Internet service providers. [AP/*USA Today*, 19 Jul
2000)
<http://www.usatoday.com/life/cyber/tech/cti244.htm>; NewsScan
Daily, 19 July
2000]

🔥 Google allows anonymous spam

Lloyd Wood <l.wood@eim.surrey.ac.uk>
Wed, 12 Jul 2000 18:23:16 +0100 (BST)

<http://services.google.com/cgi-bin/emailresults?/search?q=>

In providing an 'e-mail these results to friends' service,
Google is allowing
completely anonymous mail delivery; just delete the filled-in
search text
and go.

The risk is that this will be used for spam or for harassment;
Google
headers and footers mean that Google will get any blame. If
you're ranked
highly on a particular Google search, this becomes an obvious
and convenient
promotional tool for you: you're 'recommended by Google!'.
.

Or, if you miss anon.petit.fi, this may be good news, since
tracing the
source without contacting Google is made less straightforward.

Received: from services.exo.google.com (crawler.googlebot.com
[209.185.253.175]

(may be forged))

by ns.google.com (8.9.3/8.9.3) with ESMTTP id JAA11738
for <l.wood@iee.org>; Wed, 12 Jul 2000 09:58:25 -0700

Unlike hotmail et al, Google doesn't even append an initial Received: header providing the IP address of the originating machine or proxy; just a somewhat useless 'may be forged' warning.

I can't see this service staying in its current state long.

<L.Wood@surrey.ac.uk>PGP<<http://www.ee.surrey.ac.uk/Personal/L.Wood/>>

🔥 British law would allow police to intercept e-mail

"NewsScan" <newsscan@newsscan.com>

Wed, 19 Jul 2000 12:28:55 -0700

The British government appears likely to enact legislation that would allow law enforcement authorities to intercept personal and corporate e-mail messages and would require Internet service providers to install, at their own expense, surveillance equipment that would resend some of their customers' messages to a monitoring center run by the domestic security service, MI5. A government official argued that "the powers in the bill are necessary and proportionate to the threat posed by 21st century criminals, no more, no less." The bill has angered civil libertarians, and a spokesperson for Amnesty International in London said: "What this does is contravene a large number of fundamental rights in the European convention on human rights and other international standards, which include the right to privacy, the right to liberty, the right to freedom of

expression, and
the right to freedom of association." [*The New York Times*, 19
Jul 2000
[http://www.nytimes.com/library/tech/00/07/biztech/
articles/19britain.html](http://www.nytimes.com/library/tech/00/07/biztech/articles/19britain.html);
NewsScan Daily, 19 July 2000]

⚡ Clinton administration plans on wire taps & encryption

"NewsScan" <newsscan@newsscan.com>
Tue, 18 Jul 2000 08:49:33 -0700

A speech by White House chief of staff John D. Podesta has pleased the business community with the Administration's new software encryption policy, which will loosen export controls on encryption technology, but upset civil libertarians with the Clinton Administration's position on allowing law enforcement agencies to monitor Internet traffic. Barry Steinhardt of the American Civil Liberties Union said the government's attempt to expand wiretapping on the Internet "represents a grave threat to the privacy of all Americans by giving law enforcement agencies unsupervised access to a nearly unlimited amount of communications traffic." [*The Washington Post*, 18 Jul 2000, <http://www.washingtonpost.com/wp-dyn/articles/A57330-2000Jul17.html>;
NewsScan Daily, 18 July 2000]

⚡ ID theft finally coming to the fore

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

Thu, 22 Jun 2000 09:59:00 PDT

The RISKS archives are chock full of reported cases of people being victimized by identity theft. An article in **The Washington Post**, 13 Jul 2000, notes that the Federal Trade Commission has logged at least 20,000 phone calls since starting its toll-free hotline eight months ago. Complaints include masquerading with other people's Social Security numbers -- fraudulent loans, setting up bogus credit-card accounts, and so on. The Internet is clearing creating new opportunities, partly because of the huge amount of information available. The pending Kyl-Feinstein Senate legislation would outlaw the sale of SSNs, require better validation of credit-card address change requests, make fraud-alert notations part of credit reports once you have reported an identity theft, and provide you with free yearly credit reports (presumably only YOURS). [How about forbidding the ubiquitous use of SSNs and other easily attainable information as authenticators, not just identifiers? And while we are at it, how about getting rid of reusable passwords floating around in the clear? PGN]

⚡ Mother's maiden name as security check

"Bill Tolle" <BillTolle@ExclusiveBuyersAgents.com>

Tue, 18 Jul 2000 21:39:25 -0500

When you call many credit-card companies [and banks], they ask for your Mother's Maiden Name as verification when you want to obtain information about the account.

The State of Texas has now placed many birth records on the Internet, including the mother's maiden name.

Go to <http://userdb.rootsweb.com/tx/birth/general/search.cgi>

Enter "Smith" as Surname

Leave all other fields blank.

The search engine will return 35,072 names (first, last, and middle) with birth dates and the Mothers Maiden name (first, last, and middle) and Father's name (first, last, and middle).

Bill Tolle <BillTolle@ExclusiveBuyersAgents.com>

[Of course, the real crime is that the SSN and MMN are used as AUTHENTICATORS, as we have noted here many times. But this database really escalates the identity-theft problem. PGN]

✶ Navy to use Windows 2000 on aircraft carriers

<leveson@sunnyday.mit.edu>

Thu, 13 Jul 2000 18:30:26 -0400

A press release on 13 Jul 2000 says that "Lockheed Martin Naval Electronics systems announced that Microsoft Federal Systems is joining the Integrated Warfare Systems Team supporting the design and development of

the CVN 77,
the nuclear-powered aircraft carrier Newport News Shipbuilding
is providing
to the U.S. Navy.

Microsoft Federal Systems, based in Washington D.C., will help
design the
ship's information technology architecture based on the
company's Windows
2000 platform."

The Navy never seems to learn (remember the fiasco they had using
Windows NT on their cruisers). [Yorktown, [RISKS-19.88](#), [20.37](#)]

Prof. Nancy G. Leveson, Software Engineering Research Lab
(SERL), Aero/Astro
Dept., MIT, Cambridge, MA 02139-4307 1-617-258-0505 [http://
sunnyday.mit.edu](http://sunnyday.mit.edu)

"Information technology is becoming a key part of everything
the aerospace
and defense industry does for a living, and as the century
closes it is
computers and software that hold the keys to the future ...
Companies
that exploit information technology most effectively will be
the most
likely to dominate the aerospace landscape in the 21st
century."
David Hughes, *Aviation Week & Space Tech.*, 21/28 Dec 1998

House rejects Internet gambling bill

"NewsScan" <newsscan@newsscan.com>
Tue, 18 Jul 2000 08:49:33 -0700

The U.S. House of Representatives gave the Internet gambling
industry a
victory by failing to muster the two-thirds majority set as a

requirement by House leaders in its 245 to 159 vote on a bill to ban online casinos. The votes in favor of the ban fell 25 short of the requirement. Sue Schneider of the Interactive Gaming Council said: "It appears that cooler heads have prevailed here. We have a brand new medium we're dealing with. We don't have the same kind of borders we had before." But Rep. Robert Goodlatte (R-Va.), who sponsored the bill, scoffed at the notion that it was anti-Internet: "One way to promote the Internet is to make sure that the seamy side of life is dealt with on the Internet. Just like child pornography has to be dealt with on the Internet, so does unregulated, out-of-control, illegal gambling." [AP/*San Jose Mercury News*, 17 Jul 2000, <http://www.sjmercury.com/svtech/news/breaking/ap/docs/2063581.htm>; NewsScan Daily, 18 July 2000]

⚡ Italian crash exposes risks of online stock trading

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

Mon, 10 Jul 2000 15:54:03 -0400

Milan's stock exchange (Europe's fourth largest) opened 8 hours late on 5 Jul 2000, after corruption of the authorized-dealer database resulting from testing of a new covered-warrants market the previous evening -- evidently a maintenance glitch. Brokers claimed losses of 20 billion lire (US\$9.9M) from lost commissions. (The London exchange had an 8-hour blackout in April

2000.) [PGN-ed from

<http://www.cnn.com/2000/TECH/computing/07/10/system.crash.idg/index.html>;

⚡ DC Metro can't label rerouted trains

Wm. Randolph Franklin <wrf@ecse.rpi.edu>

Tue, 11 Jul 2000 16:02:33 -0400

On 4 Jul 2000, the Washington DC Metro (subway) system changed the routes of the several of their lines to accommodate the large number of passengers expected to see the fireworks. This was a major effort, involving taping a replacement route map over every route map in the whole system (trains and stations), printing flyers, and stationing people at the entrances to answer questions.

Unfortunately, the SW wouldn't let them couldn't change the destinations listed on the computerized signs on the trains themselves. So, the trains from Reagan airport that went to Rosslyn were labeled SPECIAL YELLOW, instead of ROSSLYN, and staff had to make frequent announcements telling what that meant.

Apparently, the list of possible destinations, which the computerized signs could display for each route, was hardcoded into the trains, and couldn't be changed.

That is, the old, cardboard, signs were more flexible than the new,

computerized signs. I'll let you draw the moral.

Wm. Randolph Franklin, Electrical, Computer, and Systems
Engineering Dept.,
Rensselaer Polytechnic Institute <rfranklin@altavista.net>

✶ Illinois man dies after utility cuts power

Bill Higgins-- Beam Jockey <higgins@fnal.gov>

Wed, 12 Jul 2000 18:18:53 -0500

I found the following story at the *Chicago Sun-Times*.
<<http://www.suntimes.com:80/output/news/vent12.html>>

> Man dies after ComEd cuts power
>
> July 12, 2000
>
> BY DAN ROZEK AND STEVE WARMBIR SUBURBAN REPORTERS
>
> An elderly Aurora man who used an electrically powered oxygen
system
> to help him breathe died in his home several hours after ComEd
shut
> off the power because he was behind in his bills.

In Aurora, Illinois, Eric Shackelford, an 81-year-old man, used
oxygen 24
hours a day to help him breathe; he suffered from "severe heart
disease."

His daughter, Renia Thomas of Chicago, claims that the power
cutoff shut his
oxygen down, and may bring a wrongful-death lawsuit against the
power
company, Commonwealth Edison.

The story reports, however, that a roommate says Shackelford had
two oxygen
systems, one of which did not depend on electrical power.

The RISKS relevance is in the dispute over record-keeping. The family says that Shackelford's doctor had sent at least two letters to ComEd asking that power not be shut off.

> A ComEd spokesman, however, said the utility had never received enough
> information to determine that Shackelford was entitled to be added to
> a list of about 1,000 customers who needed continuous electric power
> for medical equipment. ComEd files contain only one letter from a
> doctor regarding Shackelford, ComEd spokesman Don Kirchoffner said.
>
> "We would never, ever cut the power to anyone we thought was on life
> support," Kirchoffner said. [...]
> A final notice sent in June said
> Shackelford should notify ComEd if he had medical equipment that
> required electricity, and there's no record anyone contacted the
> utility, Kirchoffner said. [...]
> Kane County Coroner David Moore said it was unclear whether the power
> shutdown caused or contributed to Shackelford's death.

It would be interesting to know more about the process by which a power company keeps track of customers who are dependent on power. How do you make such a process fail-safe?

Bill Higgins Fermi National Accelerator Laboratory
<higgins@fnal.gov>

✦ Fox network misprograms time on US VCRs for a year

"Michael D. Crawford" <crawford@goingware.com>

Sat, 15 Jul 2000 11:58:26 -0700

http://dailynews.yahoo.com/h/nm/20000714/tc/life_vcr_dc_2.html

describes how Fox Broadcasting Corp. sent out a signal that programmed the time for VCRs with an automatic time setting feature to be US Pacific time for about a year, regardless of whether the VCR was located in another time zone.

The result was that VCR owners across the country found the time set on their machines wrong and they couldn't figure out why.

The problem was uncovered by the San Jose Mercury News. Apparently one is supposed to defer to local stations to set the time.

The *Mercury News* article is here:

<http://www.mercurycenter.com/svtech/news/breaking/merc/docs/001688.htm>

Apparently also a northern California PBS station reprogrammed viewers' VCRs 24 minutes fast for about two years.

> ``We don't really know how much simpler to make it,'' Tom Hantson, national product manager for Panasonic Consumer Electronics Co., a prominent VCR manufacturer, told the Mercury News. ``But no matter how simple you make it, it's not simple enough.''

Michael D. Crawford crawford@goingware.com <http://www.goingware.com>

[Also noted by Tom Van Vleck. PGN]

⚡ Company lost domain name

"Arthur J. Byrnes" <arthur@ajb.com>

Mon, 10 Jul 2000 00:39:18 -0400

>J.P. Morgan & Company (worth \$21 billion) lost its Internet connectivity on

>13 Jun 2000 because they failed to pay their \$35 bill from Network Solutions

>for their jpmorgan.com domain: three bills ignored over six weeks.

Since reading these type of stories, and not wanting to lose my 3 letter domain to the same kind of "ignorance", I have been keeping a close eye on my domain registration.

My domain was due to expire July 31, 2000 Now according to NSI's web site, here is how it should work;

>Under normal conditions, 30 days before the annual renewal fee is due,

>Network Solutions' will send an invoice to the billing contact by postal and

>electronic mail. Payment is due within 30 days. If payment is not received

>by the due date, the domain name is subject to deactivation and deletion.

>The registrant is solely responsible for ensuring that their Web Address

>remains active.

I received neither the e-mail, or the snail mail notification that NSI says

I should have. Yes, the e-mail and snail mail contact info are correct and complete.

So, my personal experience makes me wonder where the blame actually lies in these stories. I know that if I worked for a dot.com, I'd be checking all of my employer's domains expiration dates.

Arthur J. Byrnes

✶ Royal Mail claims web orders encrypted when they aren't

Gary Barnes <gkb@bofh.org.uk>

Tue, 18 Jul 2000 14:18:27 +0100

A couple of weeks ago I wanted to order a substantial quantity of stamps, and so went to the Royal Mail web site (<http://www.royalmail.com/>). I clicked on the "Business Solutions" link at the foot of their front page, and was taken to <http://www.royalmail.com/atwork/> where there's a sidebar in which "Shop" appears twice.

Following this link takes one to <http://www.royalmail.com/shop/index.htm>, "The Shop".

I then clicked on "Stamps and Envelopes for business", and started to place my order. When prompted to enter my credit card number to pay, I checked the URL of the frame containing the form asking for these details. It was <http://www.royalmail.com/shop/direct/order.asp>, and wasn't encrypted.

When I checked the "Security" link at the left of this very same page, I was

told (<http://www.royalmail.com/shop/security.htm>):

"Worried about security? For your ease of mind, all orders sent from your computer to our web servers for products featured on this Internet web site will be secured through the use of encryption technology"

In fact, there is a certificate for www.royalmail.co.uk, and I was able to place an encrypted order via <https://www.royalmail.co.uk/shop/direct/order.asp>

I contacted the webmaster to point out that their shop didn't use a secure URL, and received a reply saying that this would be fixed as soon as possible, but this hasn't been done nearly two weeks later.

The RISK here is that customers will believe a web site that says "all orders sent from your computer to our servers [...] will be secured through the use of encryption technology", especially when the organisation responsible is as "trustworthy" as Royal Mail, and then trustingly send their unencrypted card details over the Internet.

There's also the RISK that once alerted to such mistakes companies won't or can't act to fix the problem in a timely fashion, or at least remove their incorrect boasts of being "secure".

Another contributory RISK seems to be the use of relative URLs such as "direct/order.asp" instead of absolute URLs such as "https://www.royalmail.co.uk/shop/direct/order.asp".

Gary Barnes

⚡ London Underground magnetic ticket bug

<boyd.roberts@ca-indosuez.com>

Tue, 18 Jul 2000 14:24:19 +0200

When I was in London last week, I'd just gone out through the ticket barrier with my magnetic ticket. Then I re-entered because I'd seen a timetable which had some information I needed. So far, so good. When I tried to get out my ticket was refused. A London Transport employee explained to me that there was a timer on the ticket. You can't get out until either the timer expires or you find someone to let you out.

This is atrocious design. They are trying prevent you from entering multiple people with the same ticket but the timer runs in both senses; entry and exit. I guess they're just very lucky that you can't get to your destination too quickly.

It could be even worse; say there's a fire and you need to get out and the station is not staffed. Who'd get sued over that? LT? The system designers? Could be interesting / catastrophic.

The Paris Metro, RER and SNCF does this right. There's an entry timer, but it's not used to control exiting.

Boyd Roberts <boyd.roberts@ca-indosuez.com>

⚡ Man charged with breaking into NASA computers

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

Thu, 13 Jul 2000 07:14:45 -0400

A 20-year-old man was arrested Wednesday for allegedly breaking into two computers owned by NASA's Jet Propulsion Laboratory and using one to host Internet chat rooms devoted to hacking. Raymond Torricelli of New Rochelle, N.Y., was named in a five-count complaint that also charged him with sending unsolicited advertisements for a pornographic Web site and intercepting passwords and usernames traversing networks of computers owned by Georgia Southern University and San Jose State University. He was also accused of stealing credit card numbers that were used to make more than \$10,000 in unauthorized purchases. Court papers, which were unsealed in Manhattan federal court, alleged Torricelli was the head of a hacker group known as "#conflict" and that he used the name "`rolex.'" [Source: Reuters, 12 Jul 2000]

⚡ A self-referential risky accident

"Michael L. Cook" <MLCook@collins.rockwell.com>

Thu, 13 Jul 2000 15:40:25 -0500

I live in "semi-rural" Iowa, in an area where most house are on acreages mixed in and around farm-land. Neighboring houses are well in sight, but not close together as in a traditional suburban neighborhood.

The local telephone company has been laying fiber optic cable for the last couple of years for this rural area. They subcontract the trench cutting and physical cable placement to others. This morning on our neighbor's property, a man was guiding a trenching machine ("Ditch Witch") to where a trench was to be cut. The heavy morning dew made the grass slippery, and the machine slid down the side of the roadside ditch. The man tried to leap aside, but was knocked into the air by one of the tires of the rolling machine as it started its slide downhill. The man fell 10-15 feet into the ditch and landed on his back. Fortunately, the machine did not roll over him.

Also fortunately, my family and I were outside at the time, and my wife saw him fly through the air. We all started running to the scene. My wife got there first and yelled to call 911. I yelled to her to go to the neighbor's house, just a few yards away from her. I ran back to our house to also place a call just in case she couldn't. I called 911, and rescuers responded in a few minutes, and the man seemed all right, but was transported to the nearest large hospital several miles away.

However, my wife was unable to call from the neighbor's house. Why? The trenching folks had disabled the phone line in order to do their work! A co-worker of the injured man didn't seem panicky, but apparently didn't remember that he had a phone in his truck.

Risk: Don't have an accident while working on stuff you've disabled, since

you might need that equipment if you have an accident!

✂ **Re: Australian DST rules changed for Olympics (Lutton, [RISKS-20.94](#))**

<Fraser_McHarg@nag.national.com.au>

Mon, 10 Jul 2000 08:58:57 +1000

September is actually early spring in Australia, spring starts 1st September here. DST normally starts on the last Sunday of October.

Microsoft is "taking it calmly" doesn't actual inspire me. My NT machine at work has never got daylight savings time correct, although W98 has (until this year at least).

The biggest risk is not the changing of the date of daylight savings but having different states that are normally on the same timezone, or same difference, suddenly being different.

Fraser McHarg, Melbourne, Australia

✂ **Re: Software upgrade cancels train tickets (Shorrocks, [RISKS-20.94](#))**

Matt Fichtenbaum <mattf@ma.ultranet.com>

Sun, 09 Jul 2000 14:29:17 -0400

> There is no substitute for complete lack of proper testing or for
> un-necessary software changes.

I interpret that as "Complete lack of proper testing is an absolute requirement." Lose a minus sign, did we? :-)

✉ Re: UK Millennium Bridge instability (Woolf, [RISKS-20.92](#))

"Charles Arthur, The Independent" <carthur@independent.co.uk>

Tue, 4 Jul 2000 11:39:04 +0100

(It shut on the Monday having opened on the Sunday. The problems were less on the Sunday, though still noticeable to people who walked over.)

Worries that the bridge was overloaded are wrong, said Arup's Tony Fitzpatrick... It could support 5 times the maximum number of people you could stand on it, unless you started carrying people on your shoulders.

The interesting upshot of this, announced on 28 Jun, is that this really is a new phenomenon in bridge problems. It's caused by the pedestrians and the bridge acting as mutual exciters: certain spans of the bridge (it has three) have resonant frequencies around 1 Hz, which is roughly walking speed. This means that when the bridge begins moving from side to side, people move sideways to keep their balance - increasing the forces making the bridge swing.

Very nice animations of what happened (exaggerated) at http://www.arup.com/MillenniumBridge/images/videos/mode_5.avi and http://www.arup.com/MillenniumBridge/images/videos/mode_6.avi plus

explanations generally in the "engineering" section of the site (<http://www.arup.com/MillenniumBridge/>).

Interesting, of course, that they can simulate it now but not before...

Which does bear out the risks noted above. However, it wouldn't have

mattered if this was being done by computers or fusion-powered elves.

Nobody had encountered it before (apart, it is suggested by Arup, from a

Japanese stadium where the manufacturer insisted that the problems should

not be publicised for fear of losing face). So they couldn't design against

it.

⚡ Re: Another Win95/DOS interaction (Epstein, [RISKS-20.93](#))

Lloyd Wood <l.wood@eim.surrey.ac.uk>

Wed, 5 Jul 2000 23:42:43 +0100 (BST)

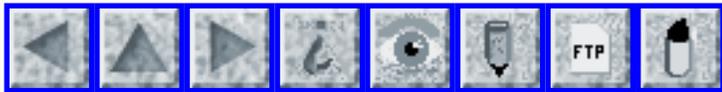
```
> Unfortunately, "/on" *really* means "sort in alphabetic order
> by the
> 8.3 short name of the file". There doesn't seem to be a way
> to tell
> the "dir" command I want it to sort the real name of the file,
> not
> the abbreviation.
```

The 8.3 "abbreviation" is in fact the real name of the file.

Windows

is hamstrung by its legacy support.

<L.Wood@surrey.ac.uk>PGP<<http://www.ee.surrey.ac.uk/Personal/L.Wood/>>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 96

Sunday 23 July 2000

Contents

- [PFIR Statement on Internet Policies, Regulations, and Control](#)
[Lauren Weinstein and Peter G. Neumann](#)
- [Info on RISKS \(comp.risks\)](#)

✦ PFIR Statement on Internet Policies, Regulations, and Control

Lauren Weinstein <lauren@vortex.com>

Sun, 23 Jul 2000 22:24 PDT

PFIR Statement on Internet Policies, Regulations, and
Control

July 23, 2000

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

Executive Summary

It is increasingly clear that the Internet, as embodied by the
World Wide
Web and a wide variety of other Net-based services and

technologies is rapidly becoming a critical underpinning and foundation to virtually every aspect of our lives, from the very fundamental to the exceedingly mundane. It is likely that few aspects of commerce, education, communications, government, entertainment, or any other facets of our daily existence will be unaffected by this exceedingly rapid change that is sweeping the globe far more rapidly than would have been anticipated only a few years ago.

These global and interconnected developments, unprecedented in human history, suggest that decisions regarding policies, regulation, control, and related Internet activities will be of crucial concern to the *entire* world's population. Consequently, the proper representation of many varied interests regarding such activities must be respected.

It is our belief that the current mechanism for making many key decisions in this regard, as embodied in The Internet Corporation for Assigned Names and Numbers, "ICANN" (<http://www.icann.org>), is proving to be inadequate to the task at hand. We believe that this is the result primarily of structural and historical factors, not the fault of the individuals directing ICANN's activities, whom we feel have been genuinely attempting to do the best possible job that they could with highly complex, contentious, and thankless tasks.

We are convinced that the Internet's future, and the future of humanity that will be depending upon it to ever increasing degrees, would be

best served
by consideration being given to the establishment of a new, not-
for-profit,
voluntary, international organization to coordinate issues of
Internet
policies and related matters. This organization would be based
on a
balanced representation of private-sector commercial and non-
commercial
interests, and public-sector interests including governmental
bodies and
organizations, educational institutions, and other enterprises.

Although the proposed course of action is expected to be
difficult, the
risks of inaction are enormous and likely to increase
dramatically in the
coming years.

The Historical Basis

The historical path that has led us to the current juncture is
well
summarized in a recent U.S. General Accounting Office (GAO)
Report
(<http://www.pfir.org/gao-icann.pdf>). It details how the late
Dr. Jon Postel,
Director of the Computer Networks Division of the USC
Information Sciences
Institute (USC-ISI), nearly singlehandedly managed many of the
core aspects
of Internet number assignments, hostname and domain management,
and related
tasks reaching back decades to the early days of the Internet's
ancestor the
U.S. Department of Defense ARPANET.

As one of the Net's earliest pioneers, he conducted this work
under
Department of Defense contracts related to the Net's ongoing
development and

support, and given that there were few (if any) commercial pressures related to the Net over most of those years, he was pretty much left alone to handle matters as he saw fit, ultimately as the IANA -- the Internet Assigned Numbers Authority. He did a remarkable job without which the development of the ARPANET and Internet would have been far less successful than they were as a result of his efforts.

Dr. Postel's untimely and unexpected death in 1998, less than two years ago, left both a professional and personal gap for many of us. It also raised the specter of many potential problems, given the rapidly changing nature of the Internet. We now see that many of these concerns were indeed well-founded. Before his death, Dr. Postel had been instrumental in the creation of ICANN, as an entity to fulfill the U.S. Federal Government mandate that Internet operational policy and control matters be fully privatized. The interim ICANN board of directors which he selected constituted itself as the formal board of the corporation after his death.

The GAO report discusses in detail the sequence of events through which various authority has been invested in the resulting ICANN non-profit corporation. While as recently as 1996 the IANA and other groups were proposing an international consortium to be based in Switzerland to deal with these issues, the existing incarnation of ICANN is headquartered in Marina Del Rey, California, in the same office building tower that has long housed the USC-ISI facilities where Dr. Postel labored

throughout the years.

The Current Situation and Problems

ICANN takes pains to describe itself as not "controlling" the Internet, but in practice the decisions and functions that it performs exert a degree of influence over existing Internet operations that may be difficult to differentiate from "control" except in a linguistic sense. However, it is certainly the case that by and large, there is no general rule of law *requiring* Internet-connected entities, from businesses to educational institutions, and from Internet Service Providers (ISPs) to individual Internet users, to conform to the structure of the existing network and the currently defined policies.

While there are technical considerations making it impractical for large portions of the network to migrate quickly to different domain naming servers and other related mechanisms, it would at least be theoretically possible, essentially by system administrators and users editing a few files on their systems. This underscores the remarkable fact that ICANN's role (as documented in the GAO report) is derived from only broad statutory authorities of various U.S. Government Agencies, since the U.S. Congress has not enacted legislation addressing these specific matters.

Unfortunately, even a few years ago it was not possible to accurately foresee the degree to which the Internet would very quickly permeate so

many aspects
of domestic and international commerce, education, privacy,
security, law
enforcement, and so many other facets of our societies. Nor was
it clear
how rapidly large commercial interests and incredibly vast sums
of money
would move into the Internet, in many cases resulting in
attempts to
redefine the network in a purely commercial context.

The resolving of the resulting tensions, problems, and disputes
present an
immense challenge that the fundamentally informal and ad hoc
nature of ICANN
does not appear well-suited to undertake. ICANN's style of
decision-making
and "making up the rules as we go" that worked so admirably as
the
ARPANET and Internet were in their relatively slow, gradual
stages of
non-commercial development now seem to be contributing to the
strains of
Internet policy, rather than alleviating them.

Some examples of these continuing problems and the resulting
troubling
changes are obvious even from the most recent ICANN meeting,
held in
Yokohama, Japan in mid-July, 2000. Even though many observers
had felt that
the registration and voting plan chosen by ICANN to facilitate
the election
of "At Large" directors was inherently flawed, it was still
alarming at this
late stage to see the ICANN board backpedaling on the election
schedule for
some of the At Large directors.

Also troubling is the manner in which the board plans to start a
new
study concerning the entire concept of At Large directors and
how they would

be handled in the future. While it is worthwhile that ICANN has apparently recognized that some of their previous decisions in this regard may be flawed, it is of concern to see such important decisions made, altered, and subjected to major reevaluations in such short order. Such rapid changes in direction are not conducive either to the confidence or the understanding of those persons in either the public or private sectors who necessarily view this process from afar.

Similarly, the contentious issue of domain names (which seems to attract much of the attention and time, but ultimately is likely to be one of the least important issues relating to the future of the Internet) still seems to be spinning like a top. While ICANN announced that new Top Level Domain Names (TLDs) would be assigned, they left the world pretty much hanging in the wind concerning most details, which were put off until later in the year.

One detail that they did establish is among the most questionable -- the assignment of a USD \$50,000 *non-refundable* "application fee" payable by any entity that wishes to be the registrar for a new TLD. While ICANN's desire to deal with organizations that would be able to provide stability to domain name handling is laudable, an essentially arbitrary fee of this nature has the effect of "locking out" organizations (especially of a non-commercial nature) who might very well be ideally suited to handling a TLD, but who don't have a spare \$50K laying around to irretrievably devote

to an application fee that might well lead nowhere. Meanwhile, concerns over the fairness of the existing domain-name resolution dispute policies continue to bubble up on a seemingly daily basis.

Again, we wish to emphasize that we consider these and similar problems to relate to the fundamental history and structure of ICANN, not to a lack of concern or positive intentions on the part of its directors. However, we feel that it has become clear that the foundation of ICANN is inappropriate for the sort of entity that is needed to appropriately lead the Internet in a direction to benefit the totality of the world's populations into the future.

A Proposal for a Different Approach

We suggest that only a *completely new*, more formally structured, not-for-profit, internationally-based organization is suited to this task, with clearly and precisely-defined delegations to represent a broad range of concerns and interests. We explicitly feel that existing domestic and international organizations, such as the Internet Engineering Task Force (IETF) or the United Nations, are unsuited to this purpose -- because they would inevitably bring too much historical "baggage" and existing conflicts to the table. An effective framework for dealing with these issues needs to start from first principles.

This new organization would exist solely for the purposes of helping to

resolve and manage the range of complex issues relating to the global Internet, many of which are impossible to even begin to effectively approach without international cooperation and broad agreements. We believe that this organization could thus play a major role towards helping to ensure that the Internet evolves in a manner to best benefit people around the world. Freedom of choice and the encouragement of diversity are extremely important factors when dealing with these issues. The organization would neither desire nor seek the power to impose outside decisions upon any national government or other governmental bodies, whose participation would be completely voluntary and who would always maintain sovereignty over their own decisions regarding the manner in which they and their citizens would access or otherwise use the Internet.

We do not intend this document as a blueprint for the detailed structure or operations of such a newly constituted organization, but rather as a starting point for further discussions and consideration of this concept -- as a first step. With that in mind, we proceed to offer some foundational assumptions regarding such an organization.

A primary tenet would be that this proposed organization be truly and *formally* international in nature. This means that the delegations, with decision-making powers, would be chosen in a formal manner from "day one" to provide balance to the deliberations amongst the many varied domestic and international entities and interest groups around the world. A

defined

procedure would also exist for the bringing of new groups and interests into the formal process in an appropriate manner.

The organization should be constituted in such a way as to not only represent the needs and desires of the existing developed countries where most Internet activity is currently taking place, but also the needs of the underdeveloped and developing worlds, who are in some cases already being thrust onto the Internet, but find themselves with few if any avenues to impact its directions or orientations. Similarly, the needs of economically-disadvantaged persons and groups in any countries must have consideration and weight in the process (relating to the aptly-named "digital divide"), not just the economically-advantaged to whom the bulk of the existing attention regarding Internet policies and development have been skewed.

The desires of the commercial arena are of course of great importance to the growth, development, and use of the Internet, but they cannot continue to be of **overriding** precedence as increasingly now appears to be the case. To that end, the organization would include delegations to balance the interests of for-profit and non-profit, commercial and non-commercial groups and persons, with all facets having a relatively equal voting share towards the outcome of deliberations. Should educational and non-profit research institutions and focused public service groups have a formal say

towards the Internet's future as well as billion-dollar for-profit corporations? We say yes.

A third balancing but **not** dictatorial element of the proposed organization would be public sector participation by domestic governments and their various institutions. While we realize that this is a controversial element, we feel that it is absolutely crucial. Privatization may be all the rage, but it is unrealistic in the extreme to expect successful management of the Internet, its resources, and the many competing concerns of the world's citizenries without at least some government involvement in the process. Neither the for-profit nor non-profit worlds can be expected to adequately fulfill this role on their own.

The lack of a formal role for governments and the interests of government agencies in the **global** process of Internet policymaking is already resulting in all manner of unfortunate and even dangerous aberrations. The national governments of many countries are already implementing unilateral rules, restrictions, and sometimes bizarre policies, many of which are nonsensical when taken in the international borderless context of the Internet. The result is confusion all around, for individual users, businesses, non-profit organizations, and everyone else. International disputes, such as the continuing disagreements between the European Union and the United States over consumer and Internet privacy policies, are another example of the problems that result when these issues

are not dealt with adequately on a continuing, developmental basis, with input from national governments *and* the other groups we've defined above, on a *cooperative* basis all throughout the process.

Attempts to keep the Internet policymaking process free of government input have often resulted in governments swooping in later, frequently with what might be characterized as "knee-jerk" reactions, often to the detriment of the Internet and its global community. It would be far better to define the participatory role of governments in the first place, and have them as part of the team, rather than as an after-the-fact "spoiler" kept on the sidelines for most of the deliberations process. They deserve to be involved, and they should be involved.

Of course, the various participatory categories as defined above are not the only manner in which the range of involved interests could be organized. Educational institutions, for example, can fall into for-profit, non-profit, public, and private classifications, suggesting other possible ways to structure or define these categories. The important point is that whatever detailed organization is chosen, it be formally structured in a manner that guarantees balanced and appropriate participation by all involved parties.

Will the creation and operation of this proposed organization be simple or without any conflict? No and no -- without doubt, it will be an extremely difficult undertaking, without any guarantee of success.

Determining the details of a fair system for representation and voting by the many diverse persons, interests, groups, and institutions who would be involved will be challenging to say the very least, and there will be many other difficult issues to resolve.

On the other hand, it is obvious that the existing process is not working, and appears to be leading us ever farther down a path of increasing conflicts, rising confusion, growing concerns, and simmering anger on the part of users and organizations -- plus ever more radical reactions. The internationally-focused, formally-balanced approach proposed herein may have a chance of helping to steer the incredible hybrid of people and machines -- the Internet -- onto a course that will benefit *all* of humanity.

The Internet is undoubtedly one of the most powerful tools that has come to pass in human history -- for good or ill. To squander it, to allow short-sighted attitudes or the self-interests of any particular groups or individuals to divert its course to the detriment of society, would earn us the condemnation of the future. How much better it would be to instead earn the future's thanks, for doing what we knew was right, when we had the opportunity to do so.

- - - - -

Lauren Weinstein
lauren@pfir.org or lauren@vortex.com or lauren@privacyforum.org
Co-Founder, PFIR - People For Internet Responsibility - <http://>

www.pfir.org

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

Member, ACM Committee on Computers and Public Policy

Peter G. Neumann

neumann@pfir.org or neumann@csl.sri.com or neumann@risks.org

Co-Founder, PFIR - People For Internet Responsibility - [http://](http://www.pfir.org)

www.pfir.org

Moderator, RISKS Forum - <http://catless.ncl.ac.uk/Risks>

Chairman, ACM Committee on Computers and Public Policy

<http://www.csl.sri.com/neumann>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 97

Thursday 27 July 2000

Contents

- [House hearing on FBI's "Carnivore"](#)
[Alan Davidson](#)
- [Fake Paypal site collects user ids and passwords](#)
[Avi Rubin](#)
- [Followup on cause of SeaLaunch rocket failure](#)
[Kenneth Basye](#)
- [Outlook bug allows self-executing Trojan horses](#)
[Kevin Poulsen](#)
- [Powergen: More credit-card info exposed](#)
[Ursula Martin](#)
- [Civilian payroll problem](#)
[Stan Niles](#)
- [The Least Mail Online](#)
[Rob Slade](#)
- [AT&T exposes account info](#)
[John Chapin](#)
- [Re: Sliced fiber-optic cable ...](#)
[Mark Richards](#)
- [Re: London Underground magnetic ticket bug](#)
[Clive D.W. Feather](#)

- [Trust and Risk in Internet Commerce, Jean Camp](#)
[PGN](#)
 - [9th USENIX Security Conference 2000](#)
[Hali McGrath](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ House hearing on FBI's "Carnivore"

Alan Davidson <abd@cdt.org>
Wed, 26 Jul 2000 23:04:40 -0400

[Written by Lina Tilman <ltilman@cdtmail.org>]

Oversight Hearing on Fourth Amendment Issues
Raised by FBI's "Carnivore" Program
Subcommittee on the Constitution, House Committee on the
Judiciary
Monday, July 24, 2000, 1:00 p.m.

Chairman Canady opened the hearing by introducing the Carnivore system as one that "isolates, intercepts and collects" information that passes through an ISP. Canady expressed hope that evaluations of the system would be based on facts instead of "irrational fears and suspicions". Canady concluded by acknowledging the potential for abuse of the system as a significant concern.

Rep. Watt briefly addressed his concern regarding Big Brother in general and the government's ability to invade citizens' privacy in particular. Watt acknowledged that such ability has been enhanced by advancements in information and communication technologies.

Rep. Hyde first noted the legitimate need of the law enforcement

to access information required for criminal investigations. Hyde then described the tension between such necessary access and the citizens' right to the "valuable commodity" of privacy.

Rep. Conyers introduced a number of questions as part of his inquiry into Carnivore's ability to "bite more than it can chew". Conyers first noted his concern regarding the applicability of the pen register authority, under which Carnivore collects transactional electronic data, to the online environment. Conyers' other concerns included the FBI's refusal to allow ISPs themselves to deliver the necessary information once a lawful order is obtained.

Rep. Hutchinson stated that while Carnivore appeared to be a minimization tool, there exist legitimate questions regarding its application. Concerns include proper monitoring of Carnivore's collection and filtering of e-mail communication. Hutchinson mentioned the Privacy Commission bill, which he co-sponsors with Rep. Moran, as an attempt to establish a body of experts who would, among other things, examine the data collection practices of law enforcement to determine whether they violate the privacy rights of the U.S. citizens.

Rep. Bachus stated that in Carnivore's case, technology appears to have "outrun the law". Bachus expressed his suspicion that criminals would easily evade the system and it would exclusively monitor the communications of law

abiding citizens. Bachus further expressed his concern regarding illegitimate access to confidential files within agencies such as the FBI.

The first panel consisted of Dr. Donald Kerr, FBI lab director, Larry Parkinson, FBI General Counsel, Kevin DiGregory, DOJ and David Green, DOJ.

Dr. Kerr introduced FBI's Carnivore as a tool, analogous to a "packet sniffer", of lawful interception of criminal communication. After being installed on a network pursuant to a court order, Carnivore collects the transactional information of its targets' e-mails; its configuration and filter settings depend on the specifics of the court order. Carnivore conducts neither broad searches nor long-term surveillance; instead, it filters out all content information and stores only the non-content "to" and "from" lines of targeted communication. Carnivore is passive on the network and is used only by a technical team of the law enforcement; in its two years of existence, it has been used very infrequently and narrowly. Dr. Kerr concluded by stating that the FBI presently plans an independent review of the system by industry and academic experts.

Mr. Parkinson testified that Carnivore is a minimization tool that operates under substantial oversight. Mr. DiGregory, in turn, argued that Carnivore is equivalent to other simple investigative tools that law enforcement uses offline.

Chairman Canady asked whether Carnivore captures the URLs of communications

with Web sites. The panelists answered that it does not, unless a URL is included in the transactional information of an e-mail. Rep. Watt appeared upset that independent review was scheduled after Carnivore has been in use for two years. A number of Members expressed distrust regarding the law enforcement's use of Carnivore under described limitations. Rep. Hutchinson asked whether the FBI has ever captured content that it then had to filter out. The panelists answered that it has not. Panelists noted that in addition to restrictions and specifications that limit data collection prior to Carnivore's activation, there exist safeguards on law enforcement's use of collected data when it is first examined and, later, at trial.

The second panel consisted of Barry Steinhardt, ACLU, Alan Davidson, CDT, Tom Perrine, Pacific Institute for Computer Security, Robert Corn-Revere, Hogan & Hartson, Matt Blaze, AT&T Labs, Stewart Baker, Steptoe & Johnson, and William Sachs, ICONN.

Mr. Steinhardt stated that Carnivore is an unprecedented maximization tool that has the potential to access all communications that pass through an ISP. Mr. Steinhardt analogized Carnivore to a digital wiretap, expressing concern that its broad access is inconsistent with restrictions set by the Fourth Amendment and the ECPA. Mr. Steinhardt noted that the FBI has a "checkered past" with regards to First and Fourth Amendment violations.

Mr. Davidson addressed the differences between transactional data in the on-

and off-line environments, noting that off-line Fourth Amendment protections do not neatly translate into online communications. Davidson showed a series of slides that displayed sample packets that Carnivore could obtain; he argued that "non-content" data that Carnivore currently accesses under a pen register or trap and trace authorization reveal a great amount the actual content of a target's communication. Davidson argued that Congress must increase statutory protections for electronic communications, raising the Carnivore authorization standard from relevant to probable cause.

Mr. Perrine noted that Carnivore is technically capable of monitoring all traffic that passes through the network. Mr. Perrine spoke about the inapplicability of telephony concepts to the online environment. He stated that the FBI's use of Carnivore lacks accountability, noting that it is impossible to monitor the system or keep track of its configurations or filters without the knowledge of its source code. Mr. Perrine argued that Carnivore represents a threat to privacy that is protected under original wiretap legislation.

Mr. Corn-Revere argued against a number of points brought up by government witnesses on the first panel. Mr. Corn-Revere appeared skeptical that the FBI would use Carnivore's capabilities in limited ways that protect individuals' privacy. He noted disconcerting implications inherent in the system's ability to switch its level of surveillance. In conclusion, Mr. Corn-Revere stated that there presently exists no way to

ensure
accountability of FBI's use of Carnivore.

Mr. Blaze argued that while the FBI operates with good intentions, it is difficult to ensure that Carnivore operates as intended. The system may inadequately filter, target the wrong individual or extract pieces of communication out of context. Mr. Blaze noted that large-scale systems such as Carnivore are problematic and tend to fail silently -- without operators' knowledge -- due to bugs, vulnerabilities and mistakes. Mr. Blaze argued that widespread publication of Carnivore's source code and architecture is the best way to ensure its soundness. [See <http://www.crypto.com/papers/openwiretap.html>; PGN]

Mr. Baker stated that communication concepts from the telephony world do not apply to electronic communication. Mr. Baker argued that it is "crazy" and "bizarre" not to acknowledge that there exists a reasonable expectation of privacy in the content-revealing "to" and "from" lines of an e-mail. He urged the Members to institute a notice requirement when a system such as Carnivore monitors e-mail communications.

Mr. Sachs testified that ISPs are capable of providing the FBI with requested communications when a lawful order exists. He noted that Carnivore represents the most intrusive method of obtaining transactional data of e-mail messages. Mr. Sachs acknowledged that albeit technically feasible, such monitoring by an ISP discourages free online communication, protected by the First Amendment, and slows down network traffic.

During the Q&A period, Davidson noted that little is known about Carnivore's precise capabilities and functions. Rep. Watt expressed concern that currently available Carnivore-like electronic surveillance systems allow anyone to monitor online traffic. Panelists noted that there exists an a-priori legal issue with the FBI's installation of Carnivore -- in the telephony world, the FBI would not be able to install, on a telephone service provider's network, a device that would monitor all passing communications. Panelists and Members appeared to agree that there must exist a notice requirement; presently, notice depends on the individual ISPs' policies. Davidson argued that two things must occur: (1) the standard for access to transactional data on the Internet must be raised, and (2) "trap and trace" must be re-defined for the online environment. Mr. Perrine noted that according to the Supreme Court, transactional data may not disclose the target's identity. Mr. Steinhardt observed that the FBI witnesses addressed the use of Carnivore in the e-mail context only; it remains unclear how the system monitors files transferred using other protocols. Furthermore, it is unclear what statutory protections govern such file transfers. Mr. Steinhardt argued that the notion and significance of non-content data has changed since CALEA was adopted, and urged the Members to consider two changes to existing surveillance guidelines: (1) judges should be given discretion in matters of online pen register and trap and

trace orders, and (2) the standard for obtaining a pen register and trap and trace must be raised for both the online and the telephony environments.

Lina Tilman, Center for Democracy and Technology
1634 Eye St. NW Suite 1100, Washington, DC 20006
202 637 9800 fax 202 637 0968
ltilman@cdtmail.org <http://www.cdt.org/>

[From EPIC Alert 7.14, 27 Jul 2000, <http://www.epic.org>, I find Testimony presented at the House Judiciary Committee hearing:

<http://www.house.gov/judiciary/2.htm>

The hearing can be viewed in its entirety over the web at:

http://www.cspan.org/technology_science/

More on the history of FBI monitoring of Internet communications and the

"digital telephony" law (or CALEA) is available at the EPIC Wiretap Page:

<http://www.epic.org/privacy/wiretap/>

PGN]

⚡ Fake Paypal site collects user ids and passwords

Avi Rubin <rubin@research.att.com>

Tue, 25 Jul 2000 15:23:18 GMT

Somebody in the Ukraine registered PayPaI.com (note the resemblance to PayPal, especially with the upper-case I [in some fonts]), then copied Paypal's HTML and sent mail to a bunch of paypal users saying 'J. Random has just transferred \$827 to you using PayPal, log in at <http://www.paypaI.com/> to claim it!' of course, as soon as you "logged in" your password was mailed to some free e-mail service. For more on the story see <http://www.msnbc.com/news/435937.asp?cp1=1> among other places.

Avi <http://avirubin.com/>

[Monty Solomon notes that Paypai.com is registered to Birykov Inc. in

South Ural, Russia, according to MSNBC: <http://www.msnbc.com/news/435937.asp>

PGN]

⚡ Followup on cause of SeaLaunch rocket failure ([RISKS-20.84](#))

<Kenneth_Basye@dragonsys.com>

Thu, 27 Jul 2000 15:45:22 -0400

According to an article at space.com, the cause of the failure in March was "a single line of code" which allowed the rocket to be launched with a valve open in the second stage, setting the stage (sorry) for a helium leak.

SeaLaunch is preparing for another launch tomorrow (July 28th). (http://www.space.com/missionlaunches/sea_launch_000714.html)

Ken Basye <kbasye@dragonsys.com>

⚡ Outlook bug allows self-executing Trojan horses

Kevin Poulsen <klp@well.com>

Wed, 19 Jul 2000 21:09:06 -0700 (PDT)

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

A newly discovered vulnerability in Microsoft's Outlook and Outlook Express programs leave thousands of computers open to attack from

malicious e-mail,
and puts the lie to the conventional wisdom that you can't get a
computer
virus if you don't open attachments.

Microsoft issued an advisory on the bug Wednesday morning, after
a
programmer announced it to the world over the Bugtraq mailing
list Tuesday.

In the advisory, Microsoft says Outlook users can eliminate the
vulnerability by upgrading to Internet Explorer 5.01 Service
Pack 1, or,
Explorer 5.5. Either upgrade will patch the hole on Windows 95,
98 or NT.
Windows 2000 users must install the Service Pack to close the
hole.

The bug is a classic "buffer overflow" error in the section of
Outlook that
parses the Date field of each incoming e-mail. By padding the
date with a
long string of characters, an attacker can escape from the area
of memory
reserved for storing it, and into a section that executes
instructions.
From there, the attacker's e-mail could secretly infect a victim
computer
with a "back door" program like Back Orifice, or instruct it to
send the
offending e-mail back out to the net like the LoveLetter virus.

The vulnerability doesn't require any attachment to the e-mail;
Outlook users
need only read a message to be hit. Outlook Express users are
even more
vulnerable, and can fall prey to malicious code without reading
the message,
or even being at their computer when it comes in.

"This has the potential to be the worst one we've seen yet,"
said Brian
Martin, a senior security engineer at Maryland-based Digital
Systems

International Corporation. "If this can execute as soon as the mail is received, oh man, that's just perfect."

Based on a hurried analysis Tuesday night, Martin said that the bug could likely be used to take control of vast numbers of machines at a time. "What if you had a mail list with thousands of people and you posted to that?," said Martin. "One well-placed e-mail and you can probably infect thousands of people with a Back Orifice or a NetBus."

Aaron Drew announced the bug to the Bugtraq mailing list on Tuesday, along with code that ostensibly demonstrates the hole. MSNBC reported that the hole was also discovered over a month ago by researchers at USSR Labs, which also boasts working exploit code. Both the news service and the security group kept it a secret while awaiting a Microsoft fix. The Microsoft advisory credits USSR Labs for reporting the bug to them, "and working with us to protect customers."

Outlook's vulnerability to running malicious code without any user interaction raises the ominous threat that a virus writer might create a fast spreading worm that would spread in the style of Melissa or last May's "ILoveYou" virus, but without the need to trick people into running hostile attachments. Experts fear that many users -- perhaps most -- will invariably fail to close the hole and will thus remain open to attack. "Nobody downloads their security patches," said Dan Schrader, an anti-virus expert at Trend Micro Tuesday. "Which is unfortunate, because it's

relatively
simple to do."

Martin warned that attackers won't be losing interest. "Between [USSR Labs] already having the code, and someone else posting follow up code to a public source, there are probably a dozen people working on their own version. And they're probably each figuring out the best ways to exploit this."

✶ Powergen: More credit-card info exposed

Ursula Martin <ursula@csl.sri.com>
Thu, 20 Jul 2000 21:03:48 -0700

The UK electricity utility Powergen advised all its online customers to change credit-card numbers after details of 7000 customers were mistakenly made available on the web in early July 2000. [Source: <http://www.guardianunlimited.co.uk/netprivacy/>]

✶ Civilian payroll problem

"Stan Niles" <sniles@arl.army.mil>
Mon, 24 Jul 2000 13:40:04 -0400

``Civilian Payroll Problem: A major systems problem with the Automated Time and Attendance Production System (ATAAPS) has resulted in a significant loss of Time and Attendance (T&A) Report data. All transactions that were

entered into ATAAPS between Saturday, 8 July 2000 and Tuesday, 18 July 2000

have been lost and are not recoverable. The lost transactions include

leave, premium pay, tour of duty changes, default job order changes, and

corrections that were made between those dates.'

I just got back from being away from work without checking in on my e-mail

for a whole week (yippee!). This is what greeted me. I don't really know

their process and I too busy digging out from the accumulated pile of mail

etc. to find out. But ten days of lost payroll data? Haven't they ever

heard of "backups"?

Stan Niles Army Research Lab <sniles@arl.army.mil>

The Least Mail Online

Rob Slade <rslade@sprint.ca>

Fri, 21 Jul 2000 09:07:26 -0800

E-mail generally works so well that we have started to take its successful

operation for granted, forgetting that delivery is still not guaranteed. As

a case in point, Sprint Canada's The Most Online service had one of its

regularly unscheduled outages last week, this time affecting incoming e-mail.

The timing was particularly unsettling to me, as a group of us were in the

final stages of negotiation with a publisher, and the discussions were being

conducted via e-mail.

From the date stamps on some late e-mail that is starting to

dribble in, the outage probably started late Wednesday night. I didn't notice anything until late Thursday, when I expected to download the usual 150 messages that would have built up in the time I had been away from Net access. Instead I couldn't get anything. Calling the Sprint support line got a recorded announcement that "some subscribers may experience some problems in obtaining incoming e-mail." Friday a dribble of e-mail started to come through, but the announcement persisted over the weekend. Wednesday a fair number of old messages started to come through, so it seems that some of the backlog is starting to clear.

However, there is no indication that I am going to get all my e-mail. In addition, during this whole outage I was sending mail from others of my accounts to the Sprint account. Of all the messages sent, some of the delayed at least six days before delivery, only one generated any kind of a bounce message or notification. (That bounce, generated at least five days after the original message was sent, stated that delivery had been impossible for at least 4 hours.) Therefore, it's quite possible that a number of people are mad at me for not responding to mail I've never seen.

Once again, the risk is that we are seeing the Internet system, dependable though it may be, as completely reliable.

(As usual, I submitted this to Sprint for their reaction before sending it out. They replied within about eight hours--confirming that the

outage had
occurred, and pointing out that their terms don't guarantee any
minimum
level of service at all :-)

In the meantime, you know where to reach me. But maybe you'd
better copy more
than one address, just to be sure :-)

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

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

⚡ AT&T exposes account info

John Chapin <jchapin@lcs.mit.edu>

Mon, 24 Jul 2000 20:00:37 -0400

I recently had occasion to call the AT&T Credit Management
Center,
1-800-532-7486.

You can type a home phone number into their voice menu system
and it will
answer back with the account standing, recent payment amounts
and dates,
without any password or other authentication. Perhaps this only
applies to
delinquent accounts (mine was, temporarily).

AT&T only recently began billing residential long distance
customers
directly here in the Boston area, rather than through Bell
Atlantic. They
appear to be new to the privacy management side of customer
accounts too.

John Chapin, Assistant Professor, MIT Laboratory for Computer

Science

545 Technology Square, Cambridge, MA, 02139, 617/253-3538, fax
617/258-8607

jchapin@lcs.mit.edu <http://sdg.lcs.mit.edu/~jchapin>

✶ Re: Sliced fiber-optic cable ... ([RISKS-20.93](#))

"Mark Richards" <mark.richards@massmicro.com>

Thu, 6 Jul 2000 09:57:16 -0400

The same thing happened in our town - a much smaller scale - but the poor response of our phone service semi-monopoly Bell Atlantic is worth noting:

Here in Massachusetts, and perhaps in other states in the US, we have something called "Dig Safe". It's both an admonition for the brain dead and an actual service for identifying buried utilities. With a simple phone call, Dig Safe coordinates the identification and marking of buried utilities so that excavators are not electrocuted or blown up.

In our small community someone either forgot to call them or the marking was incorrect. They plunged a backhoe through a Bell Atlantic buried phone cable and "disrupted" service to a few thousand customers for several days. It was an "old" cable - the wires weren't colour-coded - making the wire-matching task extremely impossible.

The really ugly part of the story is that no one, particularly Bell Atlantic, bothered to notify the local public-safety agencies. Their lame

excuse, following this debacle, was that "the police should have known, considering we requested an officer at the scene for traffic control". The "accident" left thousands without access to emergency services and the emergency services were not given proper notification to employ a backup plan.

By the way, the backup plan has already been thoroughly tested. Thanks to the incompetence of Bell Atlantic, our 911 emergency service has been knocked out twice in the past several months. Each time it's blamed on "defective equipment".

These problems continue, while our Public Utilities Commission sleeps at the switch. The only time they wake up is when Bell wants a raise.

Mark Richards <mark.richards@massmicro.com>

✶ Re: London Underground magnetic ticket bug (Boyd Roberts, [RISKS-20.95](#))

"Clive D.W. Feather" <clive@demon.net>

Thu, 27 Jul 2000 10:27:24 +0100

Actually, the risk here is in misunderstanding the system. The system as a whole (not just the automated gate) worked exactly as designed.

The ticketing gates have 40 or 50 heuristics for detecting problems and fraud. If the gate is unhappy with the ticket presented, it displays the message "Seek Assistance" and a code number that the staff can

use to
determine what the problem is.

The staff member at the barrier line can apply much more intelligence to the situation than a machine can. In particular, if you talk to railway staff you'll discover that they soon acquire a "sixth sense" of when people are trying to fiddle and when they are being honest. There are also various "trick" questions they can ask.

Mr Roberts was caught by the "in-out-in" detector. This applies *at a station*. It is quite possible to exit at a *different* station before the timer (15 minutes, I think) expires, because this detector will not then apply.

>It could be even worse; say there's a fire and you need to get out and the
>station is not staffed.

The barrier line *MUST* be staffed at all times. If the member of staff has to leave for some reason, he or she *MUST* deactivate the system, which opens all the gates. This is a Health and Safety issue, and LU would be fined heavily if caught breaking it.

>The Paris Metro, RER and SNCF does this right. There's an entry timer, but
>it's not used to control exiting.

The Paris Metro is a flat fare system, so there's no need for ticket checks on exit. The situation isn't exactly comparable.

Clive D.W. Feather <<http://www.davros.org>> <clive@demon.net>
+44 20 8371 1138

✦ Trust and Risk in Internet Commerce, Jean Camp

<"Peter G. Neumann">

Mon, 24 Jul 2000 16:59:48 -0400

Trust and Risk in Internet Commerce

L. Jean Camp

MIT Press, 2000

292 pp., ISBN 0-262-03271-6

<http://mitpress.mit.edu/promotions/books/CAMTHF99>

As Internet-based commerce becomes commonplace, it is important that we examine the systems used for these financial transactions. Underlying each system is a set of assumptions, particularly about trust and risk. To evaluate systems, and thus to determine one's own risks, requires an understanding of the dimensions of trust: security, privacy, and reliability.

In this book Jean Camp focuses on two major yet frequently overlooked issues in the design of Internet commerce systems--trust and risk. Trust and risk are closely linked. The level of risk can be determined by looking at who trusts whom in Internet commerce transactions. Who will pay, in terms of money and data, if trust is misplaced? When the inevitable early failures occur, who will be at risk? Who is "liable" when there is a trusted third party? Why is it necessary to trust this party? What exactly is this party trusted to do? To answer such questions requires an understanding of

security, record-keeping, privacy, and reliability.

The author's goal is twofold: first, to provide information on trust and risk to businesses that are developing electronic commerce systems; and second, to help consumers understand the risks in using the Internet for purchases and show them how to protect themselves. Rather than propose a single model of an Internet commerce system, the author provides the information and insights needed by merchants and consumers as they develop the Internet for commerce.

L. Jean Camp is Assistant Professor at Harvard University's Kennedy School of Government.

9th USENIX Security Conference 2000

Hali McGrath <hali@usenix.ORG>

Wed, 26 Jul 2000 18:57:04 GMT

9th USENIX Security Symposium 2000 Conference August 14 - 17, 2000 Denver, Colorado, USA Conference URL: <http://www.usenix.org/events/sec2000>

Presentations by top notch instructors and industry experts such as: Avi Rubin, Daniel Geer, Tina Bird, Brad Cox, Char Sample, Jim Duncan, Rik Farrow, and Marcus Ranum, Ian Goldberg, Suelette Dreyfus, Mudge, and Mark Chen. Keynote Speaker Dr. Blaine Burnham, Director of the Georgia Tech Information Security Center and former NSA program manager. Full program details and registration are available online at

<http://www.usenix.org/events/sec2000>.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 20: Issue 98

Monday 31 July 2000

Contents

- [San Mateo health system upgrade is a downer](#)
[PGN](#)
- [Scientists spot Achilles' heel of the Internet](#)
[Dave Farber](#)
- [Booming computer firms are running out of power](#)
[Doneel Edelson](#)
- [Stephen King's not scared of trusting online readers](#)
[NewsScan](#)
- [The paperless benefits plan](#)
[Greg Compestine](#)
- [When what you see isn't what you get](#)
[Lloyd Wood](#)
- [Computer crash caused loss of cab schedule](#)
[Jacob Palme](#)
- [Re: Bloat Dissections II](#)
[Jonathan Guthrie](#)
- [Re: The Least Mail Online](#)
[Nick Andrew](#)
- [Re: London Underground magnetic ticket bug](#)
[Boyd Roberts](#)

[Clive Feather](#)

● [Re: AT&T exposes account info](#)

[Dima Maziuk](#)

● [Susan villages](#)

[Mark Brader](#)

● [Info on RISKS \(comp.risks\)](#)

✂ **San Mateo health system upgrade is a downer**

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

Fri, 28 Jul 2000 21:29:33 PDT

San Mateo County has spent \$35 million thus far on a new Health Services

computer system (now two-years old) that was expected to integrate 40

different stovepipe entities that previously were unable to communicate with

one another. Over the past few months, the system has been so unreliable

that it could not even send out medical bills. The backlog of account

receivables is now more than \$40 million. Blame is being distributed among

poor initial outside advice, a sudden cut in anticipated money, and damaging

turnover in consultants. The costs are about double what had been budgeted.

[Source: Article by Mark Simon, *San Francisco Chronicle*, 25 July 2000, A17]

As an aside that seems relevant to many other situations if not to this one,

outsourcing of responsibilities (from requirements to design to implementation to operation and maintenance) is increasingly popular, but

doomed if you don't have serious in-house competence to understand what is

being outsourced.

⚡ Scientists spot Achilles' heel of the Internet

Dave Farber <farber@cis.upenn.edu>

Mon, 31 Jul 2000 06:50:38 -0400

[From Dave Farber's wonderful IP distribution. PGN]

The complex structure of the Internet makes it resistant to errors or failure but it is also its Achilles' heel [...]. Because the system is so varied, if one or more nodes -- the crossroads through which Internet data travel -- goes down it has very little impact. But researchers at Notre Dame University in Indiana ... have found if the networks with the most highly connected nodes were attacked by cyberterrorists, it could fragment the Web into isolated parts. [Excerpt from an article by Patricia Reaney, <http://www.zdnet.com/zdnn/stories/news/0%2C4586%2C2607716%2C00.html>, Reuters, 26 Jul 2000]

[But the Internet is a well-heeled beast: it has MANY Achilles' heels. PGN]

⚡ Booming computer firms are running out of power

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

Tue, 11 Jul 2000 09:45:20 -0400

Companies in Silicon Valley, California, are being forced to

build private power stations amid growing evidence that there is not enough electricity in America's grid to drive the booming high-tech industry. US demand has grown by 35% in the past 10 years. [Is that all?] More than 10% of all US power is for computers and related stuff. The Internet is making it even more of a problem. According to Karl Stahlkopf of the Power Research Institute, "You may think electronic gadgets can't use much electricity. In fact, when you look at the servers and the computers that back up the wireless Palm Pilot for example, you'll find it has the electrical load equivalent of a refrigerator." [PGN-ed from an article by Simon Davis, electronic Telegraph, 11 Jul 2000]

[Another item from Doneel noted an Associated Press article by Nicholas

K. Geranios, Power rates in West jolting economy, 10 Jul 2000, discussing

the effects of a sudden large hike in the cost of electric power on the

West coast -- including cases of rates being multiplied by a factor of

40 in one case. PGN]

⚡ Stephen King's not scared of trusting online readers

"NewsScan" <newsscan@newsscan.com>

Mon, 24 Jul 2000 09:21:22 -0700

He's back. Horror writer Stephen King has now used his Web site (www.stephenking.com) to post the first two installments of his new novel

"The Plant," which is about a "vampire" plant that takes over a

publishing

company. The material will be posted as pdf files, and readers will be

trusted to pay the author a dollar to download it. If King receives payment

for at least 75% of the downloads, he will continue with his plans to post

the remainder of the book on the Web. People in the publishing industry are

skeptical. Literary agent Mort Janklow says that King is "a fellow sitting

up in Maine having fun, but it's not a way to run a business."

And National

Writers' Union president Jonathan Tasini says, "You still need a lot of

money and power to promote a book. The same people who already make a good

living at the top of the bestseller list may have another way to sell, but I

don't believe there will be dramatic change for other authors."

[AP/[San Jose] *Mercury News*, 24 Jul 2000; NewsScan Daily, 24 July 2000

<http://www.sjmercury.com/svtech/news/breaking/ap/docs/2303131.htm>]

The truth about e-books

Despite the hoopla surrounding the e-publishing of Stephen King's novella,

"Riding the Bullet," the truth is that most of the 500,000 electronic copies

distributed were purchased by Amazon and Barnesandnoble.com, which then gave

them away, and many other copies downloaded were simply "experiments" by

people who wanted to see if the technology worked. According to a survey of

3,000 subscribers conducted by the Book Report Network, only 1%, or 5,000,

of those who downloaded King's first e-book actually read it.

"No reader is

asking for e-books," says Book Report Network CEO Carol Fitzgerald. "This

is not the Sony Walkman." Publisher Simon & Schuster, which distributed the novella, disputes the Book Report sampling. [*Los Angeles Times*, 24 Jul 2000 <http://www.latimes.com/business/20000724/t000069317.html> NewsScan Daily, 24 July 2000]

✈ The paperless benefits plan

"Greg Compestine" <gmc333@my-deja.com>
Mon, 10 Jul 2000 15:42:48 -0700

Last week I received an e-mail informing me that annual enrollment for benefits at my company would now be handled on the Internet. The e-mail included a login ID and password for use at the enrollment Web site but, oddly enough, not the URL for the Web site. Web enrollment is mandatory.

The e-mail contained an attached memo in MS Word format (itself wrought with RISKS). The memo in the e-mail was entitled "Read this to find out how you can win cool stuff courtesy of _____ HR!" (Company named deleted.) It goes on to say that "This will enable you to complete open enrollment on-line, view your enrollment elections and tax withholding information anytime, change your address, change your 401(k) contributions, add dependents or beneficiaries, and soon you will be able to view your pay stub here too."

I sent off a complaint about having so much data accessible on the Web. Today there were several developments.

First I discovered that I was not on the company-wide mailing list used to distribute announcements about benefits.

Then I received a reply to my complaint that the company was "sensitive to the security issues" and described two conflicting security measures. without a URL to rule out possibilities, either:

- a) the benefits Web server is behind the corporate firewall, where its security is administered by a third-party sys-admin shop, or
- b) the Web server is on a third party machine where we have no direct control over the security arrangements. (I'm not sure which alternative is worse.)

Is there any kind of audit or accrediting that Web sites can go through to verify at least minimal security arrangements? If so, I'd really like to know about them.

Among the RISKS I can list:

- 1) the company's jumping into this whole hog, without an apparent backup plan, or alternatives for people who don't want their entire employment record and benefits package hanging out in inherently insecure and unreliable Web space.
- 2) The login and passwords sent out by e-mail could be intercepted; they were in no way protected.
- 3) The format of the logins and passwords make it extremely easy to guess others. (NOT the first time I've encountered this here. The

third party

company responsible for sys admin has a habit of assigning
incredibly
obvious passwords based on the user's name.)

4) Once guessed, a user ID and password could at a minimum
provide for a
denial of service attack on an individual. I don't know (and
I hope I
don't have to find out) what procedures are in place for
changing or
recovering a password.

5) Using Web enrollment has been made into a lottery game with
prizes, which
causes me to wonder if we're really supposed to take any of
it seriously.

6) Overreliance on Internet technology has already caused me to
miss out on
receiving some important information on the benefits package.

7) The deadlines for enrollment obviously assume that there
won't be any
major glitches in the system. "You must enroll by 7/31 or
risk having
your benefits canceled." Yet just two months ago, when my
company moved
the employee stock purchase plan to Web-based administration,
glitches
caused several weeks delay in enrollment for many people.

⚡ When what you see isn't what you get

Lloyd Wood <l.wood@eim.surrey.ac.uk>

Mon, 31 Jul 2000 18:36:48 +0100 (BST)

One of our web users seems to have had a lot of trouble with
broken links in
his personal webpages on our Apache webserver over the last

couple of years.

Instead of / as a directory terminator, he'd have \. Or he'd have bizarre stuff like /\Directory\ instead of /Directory/ in his broken links.

I'd put it all down to him being a Microsoft fanboy who didn't know what he was doing; after all, he was generating the HTML pages using Microsoft Word, and therefore deserved everything he got.

(bugs in Frontpage such as leaving in local file:c:\\\ urls for images, so only the author gets to see incredibly fast-loading images when he checks his composed pages, are well-known.)

However, I had occasion to use Microsoft's Internet Explorer 5.5 today. So, I went to view his pages to see the world through his eyes.

And, through his eyes, everything worked just fine, as if there were no backslashes there at all. Every known-to-be-broken link did just the right thing. Which was odd, because I knew the links in the pages stored on our Apache server hadn't changed.

So I viewed source in IE, and discovered... no backslashes. IE *stripped out or converted the backslashes* before rendering the source to screen - even before rendering the source to 'view source'.

The user wouldn't know the backslashes were there, because IE was *deliberately hiding and converting them* for him, presumably in order to compensate for the html rendering deficiencies of other Microsoft products - and interoperability with non-Microsoft browsers be damned. The

user
thought he was doing a good job, based on checking using the
tools in front
of him.

If you view source, you expect to see the actual source, and not
a
prefiltered version. This filtering is clearly a risk in that it
allows
behaviour that would previously have been clearly exposed as
bugs in the
composing products to stay, unnoticed and uncorrected, because
it means you
can't trust the tool you're using, and because it screws up
interoperability
testing. (Which, because IE comes from Microsoft, is hardly a
surprise.)

<L.Wood@surrey.ac.uk>PGP<<http://www.ee.surrey.ac.uk/Personal/L.Wood/>>

✶ Computer crash caused loss of cab schedule

Jacob Palme <jpalme@dsv.su.se>
Sun, 30 Jul 2000 10:45:43 +0200

When I was leaving home to travel to the IETF meeting in
Pittsburgh next
week, the pre-ordered taxi did not come on time. After waiting
five minutes,
I phoned them and was told that they had had a computer crash
during the
night, and all pre-bookings had been erased. They sent a cab
when I called,
and I arrived at the airport 20 minutes late (the bus on the
second leg on
the journey was also delayed). I did catch my flight, but with
criticism
from the ticket checkers that I was late. I did not have time to

change

money at the airport as I had planned. So my loss was only perhaps 10-15 dollars in more expensive credit card buys as compared to cash buys. Others may have been less lucky. The flight was not delayed, this airline obviously did not feel that this was a reason for delaying the flight.

I do not know of the cause of the crash, so one can only guess:

- 1: The computer stopped, and no one on a Saturday night knew how to reboot it.
- 2: Software failure.
- 3: Random disk error in the data base files made them unusable.
- 4: A real disk crash had occurred.

One wonders about

- 1: Did they have adequate instruction on error handling and education to their operators, or a system with a software specialist on call?
- 2: Was the software tested well enough?
- 3-4: Did they use some disk redundancy system capable of continuing running if a single disk crashes or a single disk error occurs?

In particular, disk redundancy systems and fail-safe computers (not 100 % safe, of course) do exist, but how often are they used when they should have been used? A time-scheduling system, whose breakage would delay hundreds of people by 20 minutes in going to the airport, would that be a system which should have a disk redundancy system? Perhaps the companies marketing such

systems could use this example as a basis for selling their software to companies who do not understand the risks and what can be done about them.

The cab company involved was "Flygbusstaxi" -- which is a shell company for several other cab companies providing the actual transportation services

Jacob Palme <jpalme@dsv.su.se> (Stockholm University and KTH) for more info see URL: <http://www.dsv.su.se/jpalme/>

✂ Re: Bloat Dissections II (Liber, [RISKS 20.92](#))

Jonathan Guthrie <jguthrie@brokersys.com>

Sun, 16 Jul 2000 11:04:10 -0500 (CDT)

> The real cost isn't in the 10-minute fix; it's in verifying the 10-minute
> fix. That is the RISK.

NO!

The real risk is using an invalid analysis to reach a bogus conclusion.
THAT is the risk.

How is Mr. Liber's analysis invalid? Well, off the top of my head and in no particular order, he makes an "apples to oranges" comparison, adds costs to the bloat removal process that aren't necessarily there, does not fully account for the costs of bloat, and assumes facts not in evidence.

When comparing the costs of the bloated software to the cost of removing

the bloat, Mr. Liber compares the amount of time required to remove the bloat with the amount of money required to store the bloated software on a hard disk. Obviously, he should compare time against time or money against money, but he cannot compare money against time unless the conversion between the two is known. This is especially true when he concludes:

> Your fix is worth, at best, a fraction of a cent to your customer. If this > causes you to slip shipping by even one day, you've made a bad decision to > work on it.

This begs the questions: How much is a one-day slip in the release of a commercial application worth to a customer? Mr. Liber appears to assume that it costs quite a bit. However, it is not that hard for me to imagine a situation where a single day slip in the release date of an application has a significant NEGATIVE cost to a particular end user. In no case is the answer to my question large and positive for end users of mass-market software. Waiting an additional day for the next version of "Word" simply doesn't cost the user very much.

How is the cost of removing bloat overstated? Well, because the regression testing mentioned in Mr. Liber's message would need to be done anyway as part of the release process for any new software version. Since removing the bloat would, most likely, be done before the application began the long road through the QA department (assuming, of course, that there

IS a "long road through the QA department" which is another discussion for another time) then there is NO additional testing cost associated with removing the bloat.

Perhaps the strongest disagreement I have with Mr. Liber's message is the attempt to argue the costs of bloat out of existence. The cost of bloated software is more than just a few cents worth of hard disk space. You see, when used, that software needs to be transferred from the hard disk into main memory. While the capacities of hard disks have expanded rapidly, the time required to transfer large files from a hard disk has not decreased quite so much and the time is not linear with the size of the software to load: Programs that are twice as large typically take more than twice as long to load.

And this time adds up. If bloat causes the software to take an average of one additional second to load and the software has an average of 100,000 uses daily over the entire customer base, then over an 18-month lifespan the product wastes 1545 man-days of time just waiting for the software to load. Compare that to a couple of weeks for a couple of guys and you get quite a different answer for whether it is worth the effort to reduce the bloat than that presented in the original message. Especially in light of the fact that, if the total production run for the software is 1,000,000 units, the bloatware reduction effort takes 100 man-weeks, and each man-hour costs

\$100, the total increase in the cost of each unit as a result of that bloatware effort is 40 cents.

Nor is the time required to transfer the program off the hard disk the only cost that was missed in the original analysis. In addition to the cost of the additional hardware required to run ever more bloated applications, you've got to include the downtime required to upgrade the hardware to satisfy the requirements of software that won't run on older hardware. If the application lives on a file server, then you've also got wasted network bandwidth and wasted time to periodically upgrade the network to handle the additional load.

Further, it seems likely to me that the larger an application is, the more likely it is to exhibit poor locality of reference which means that bloated applications make less effective use of semiconductor cache and require more effort to make effective use of virtual store. The net effect of bloatware is, therefore, to make the entire computer system perform more poorly, even on higher-performance computers of recent manufacture.

The facts not in evidence? Well, Mr. Liber's message implies that the decision to release bloatware is always the result of a careful analysis, made by the software vendors, of the relative costs and benefits. If only that were the case! There is a profound difference between a conscious choice to reduce the cost of a product by not reducing the size of an application and releasing bloatware because of ignorance or

apathy. Use of the additional resources available in recently manufactured microcomputers is allowable. Waste of those same resources is, to me, unacceptable, and waste is certainly what it appears, to me, to be.

In fact, the part that really makes me angry is the fact that the benefits of not reducing the bloat are reaped solely by the software vendor, but the costs are borne solely by the consumer. This shows a disrespect of the end user that borders on contempt. I don't like to be held in contempt by those who want me to give them money.

One opinion, worth what you paid for it.

Jonathan Guthrie, Brokersys, 12703 Veterans Memorial #106,
Houston, TX
77014, USA +281-580-3358 <http://www.brokersys.com/>
jguthrie@brokersys.com

✶ Re: The Least Mail Online ([RISKS-20.97](#))

Nick Andrew <nick@zeta.org.au>

29 Jul 2000 16:42:52 +1000

> ... Sprint Canada's The Most Online service had one of its regularly
> unscheduled outages last week, this time affecting incoming e-mail.

There is a related risk here - the risk of assuming that you are dependent on a provider for E-mail services. It is a relatively simple matter, given a static IP address, your own domain name and a (semi-)permanent

link,
to run your own mail server which will allow you to have some
control
over E-mail reliability. So long as your server is actually
connected
to the Net, (which you can test) the ISP's mail server is now
out of
the loop as E-mail can pass directly from the source to your
destination.

Nick, Pacific Internet +61-2-9253-5762 <http://www.zeta.org.au/>

⚡ Re: London Underground magnetic ticket bug (Feather, [RISKS-20.97](#))

<boyd.roberts@ca-indosuez.com>

Mon, 31 Jul 2000 10:56:11 +0200

> ... If the member of staff has to leave for some reason, he or
she ***MUST***
> deactivate the system, which opens all the gates. This is a
Health and
> Safety issue, and LU would be fined heavily if caught breaking
it.

You never fix bad design by kludging around it. That, by
definition, proves
that it was badly designed. You design it right and you design
it so that
it's fail safe.

Boyd Roberts <boyd.roberts@ca-indosuez.com>

⚡ Re: London Underground magnetic ticket bug (Roberts, [RISKS-20.98](#))

"Clive D.W. Feather" <clive@demon.net>

Mon, 31 Jul 2000 13:50:56 +0100

> You never fix bad design by kludging around it. [...]

"Don't let people get trapped behind unmanned gates" is a bad design?

I hope you don't design life-critical systems.

Clive D.W. Feather <clive@demon.net> +44 20 8371 1138 <http://www.davros.org>

🔥 Re: AT&T exposes account info (Chapin, [RISKS-20.97](#))

Dima Maziuk <dmaziuk@crosswinds.net>

Fri, 28 Jul 2000 23:44:01 -0500

> You can type a home phone number into their voice menu system and it will

> answer back with the account standing, recent payment amounts and dates,

> without any password or other authentication. ...

Were you calling from home? -- I[1] would check if the number you typed

matches CLI[2] we get from the exchange when answering your call. If it does

there's no reason for extra security: whoever's calling is already inside

your house...

Telstra[3] voice mail works the same way: if you call from home you're

asked for PIN, if you call from somewhere else you have to type in

mbox number and pin[4].

[1] my last job was IVR programming

[2] caller line id
[3] main carrier in .au
[4] of course you don't know your mbox number -- you've always called from home before and nobody ever told you your mbox has a number...

Dima

[Also noted by Jonathan Kamens, who added:
Sure, there's the possibility that someone without legitimate need for that data could call AT&T from your home telephone, but that's not a particularly likely scenario or one with much risk associated with it.]

✶ Susan villages

Mark Brader <msb@vex.net>
Sun, 30 Jul 2000 00:08:35 -0400 (EDT)

* From: Frances Kemmish <archaeo@iconn.net>
* Newsgroups: alt.usage.english
* Subject: Re: Susan
* Date: Wed, 26 Jul 2000 08:50:17 -0400

John Steele Gordon wrote:

> Alex Chernavsky wrote:
> > Frances Kemmish wrote, quoting Finest Hour: The Battle of Britain:
> >
> > >A fuller quotation, from page 179 of the US edition:
> > >"But a forced peace, rather than Panzers in Susan villages,
> > >was the most likely way Britain might lose the war in 1940."
> >
> > Pandas in Sichuan villages? Certainly, that strategy would have been
> > a less likely way for Britain to lose the war.
>

> Panzers in Sussex villages, however, would have done the trick.

I think this is the answer; it fits both the references to "Susan".

I assume that the US edition was spell[ing]-checked using the same spell[ing]-checker which I have - it offered me "Susan" as first replacement for "Sussex".

Fran

[This thread included a variety of other computer-aided misspellingz. PGN]



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