

<http://catless.ncl.ac.uk/Risks/24.01.html>

<http://catless.ncl.ac.uk/Risks/24.02.html>

<http://catless.ncl.ac.uk/Risks/24.03.html>

<http://catless.ncl.ac.uk/Risks/24.04.html>

<http://catless.ncl.ac.uk/Risks/24.05.html>

<http://catless.ncl.ac.uk/Risks/24.06.html>

<http://catless.ncl.ac.uk/Risks/24.07.html>

<http://catless.ncl.ac.uk/Risks/24.08.html>

<http://catless.ncl.ac.uk/Risks/24.09.html>

<http://catless.ncl.ac.uk/Risks/24.10.html>

<http://catless.ncl.ac.uk/Risks/24.11.html>

<http://catless.ncl.ac.uk/Risks/24.12.html>

<http://catless.ncl.ac.uk/Risks/24.13.html>

<http://catless.ncl.ac.uk/Risks/24.14.html>

<http://catless.ncl.ac.uk/Risks/24.15.html>

<http://catless.ncl.ac.uk/Risks/24.16.html>

<http://catless.ncl.ac.uk/Risks/24.17.html>

<http://catless.ncl.ac.uk/Risks/24.18.html>

<http://catless.ncl.ac.uk/Risks/24.19.html>

<http://catless.ncl.ac.uk/Risks/24.20.html>

<http://catless.ncl.ac.uk/Risks/24.21.html>

<http://catless.ncl.ac.uk/Risks/24.22.html>

<http://catless.ncl.ac.uk/Risks/24.23.html>

<http://catless.ncl.ac.uk/Risks/24.24.html>

<http://catless.ncl.ac.uk/Risks/24.25.html>

<http://catless.ncl.ac.uk/Risks/24.26.html>

<http://catless.ncl.ac.uk/Risks/24.27.html>

<http://catless.ncl.ac.uk/Risks/24.28.html>

<http://catless.ncl.ac.uk/Risks/24.29.html>

<http://catless.ncl.ac.uk/Risks/24.30.html>

<http://catless.ncl.ac.uk/Risks/24.31.html>

<http://catless.ncl.ac.uk/Risks/24.32.html>

<http://catless.ncl.ac.uk/Risks/24.33.html>

<http://catless.ncl.ac.uk/Risks/24.34.html>

<http://catless.ncl.ac.uk/Risks/24.35.html>

<http://catless.ncl.ac.uk/Risks/24.36.html>

<http://catless.ncl.ac.uk/Risks/24.37.html>

<http://catless.ncl.ac.uk/Risks/24.38.html>

<http://catless.ncl.ac.uk/Risks/24.39.html>

[**http://catless.ncl.ac.uk/Risks/24.40.html**](http://catless.ncl.ac.uk/Risks/24.40.html)

<http://catless.ncl.ac.uk/Risks/24.41.html>

<http://catless.ncl.ac.uk/Risks/24.42.html>

<http://catless.ncl.ac.uk/Risks/24.43.html>

<http://catless.ncl.ac.uk/Risks/24.44.html>

<http://catless.ncl.ac.uk/Risks/24.45.html>

<http://catless.ncl.ac.uk/Risks/24.46.html>

<http://catless.ncl.ac.uk/Risks/24.47.html>

<http://catless.ncl.ac.uk/Risks/24.48.html>

<http://catless.ncl.ac.uk/Risks/24.49.html>

<http://catless.ncl.ac.uk/Risks/24.50.html>

<http://catless.ncl.ac.uk/Risks/24.51.html>

<http://catless.ncl.ac.uk/Risks/24.52.html>

<http://catless.ncl.ac.uk/Risks/24.53.html>

<http://catless.ncl.ac.uk/Risks/24.54.html>

<http://catless.ncl.ac.uk/Risks/24.55.html>

<http://catless.ncl.ac.uk/Risks/24.56.html>

<http://catless.ncl.ac.uk/Risks/24.57.html>

<http://catless.ncl.ac.uk/Risks/24.58.html>

<http://catless.ncl.ac.uk/Risks/24.59.html>

<http://catless.ncl.ac.uk/Risks/24.60.html>

<http://catless.ncl.ac.uk/Risks/24.61.html>

<http://catless.ncl.ac.uk/Risks/24.62.html>

<http://catless.ncl.ac.uk/Risks/24.63.html>

<http://catless.ncl.ac.uk/Risks/24.64.html>

<http://catless.ncl.ac.uk/Risks/24.65.html>

<http://catless.ncl.ac.uk/Risks/24.66.html>

<http://catless.ncl.ac.uk/Risks/24.67.html>

<http://catless.ncl.ac.uk/Risks/24.68.html>

<http://catless.ncl.ac.uk/Risks/24.69.html>

<http://catless.ncl.ac.uk/Risks/24.70.html>

<http://catless.ncl.ac.uk/Risks/24.71.html>

<http://catless.ncl.ac.uk/Risks/24.72.html>

<http://catless.ncl.ac.uk/Risks/24.73.html>

<http://catless.ncl.ac.uk/Risks/24.74.html>

<http://catless.ncl.ac.uk/Risks/24.75.html>

<http://catless.ncl.ac.uk/Risks/24.76.html>

<http://catless.ncl.ac.uk/Risks/24.77.html>

<http://catless.ncl.ac.uk/Risks/24.78.html>

<http://catless.ncl.ac.uk/Risks/24.79.html>

<http://catless.ncl.ac.uk/Risks/24.80.html>

<http://catless.ncl.ac.uk/Risks/24.81.html>

<http://catless.ncl.ac.uk/Risks/24.82.html>

<http://catless.ncl.ac.uk/Risks/24.83.html>

<http://catless.ncl.ac.uk/Risks/24.84.html>

<http://catless.ncl.ac.uk/Risks/24.85.html>

<http://catless.ncl.ac.uk/Risks/24.86.html>

<http://catless.ncl.ac.uk/Risks/24.87.html>

<http://catless.ncl.ac.uk/Risks/24.88.html>

<http://catless.ncl.ac.uk/Risks/24.89.html>

<http://catless.ncl.ac.uk/Risks/24.90.html>

<http://catless.ncl.ac.uk/Risks/24.91.html>

<http://catless.ncl.ac.uk/Risks/24.92.html>

<http://catless.ncl.ac.uk/Risks/24.93.html>

<http://catless.ncl.ac.uk/Risks/24.94.html>



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 1

Wednesday 10 August 2005

Contents

- [Russian remote controlled submarine failure](#)
[Martyn Thomas](#)
- [Caltrans screwup](#)
[PGN](#)
- [Lightning causing problems for lightning-detection system](#)
[Klaus Johannes Rusch](#) [PGN](#)
- [Navy jet has severe brake failure](#)
[PGN](#)
- [US Navy to drop paper charts](#)
[Scott Peterson](#) [PGN](#) [Scott Peterson](#)
- [Social Security Administration sends cards to the wrong place](#)
[Jonathan Kamens](#)
- [German social services software drops changes](#)
[Debora Weber-Wulff](#)
- [Hermann Chinery-Hesse and software in Ghana](#)
[James H. Haynes](#)
- [Greeting answering machine!](#)
[R H Draney via Mark Brader](#)

- [Every odd digit of number A, even digit of number B](#)
[Dan Jacobson](#)
 - [The risks of cell-phone auto-spellers](#)
[William Colburn](#)
 - [Credit-card obfuscation](#)
[William Colburn](#)
 - [Re: Car computer systems at risk to viruses](#)
[Adam Laurie](#)
 - [Re: Increasing sophistication of phishing spammers](#)
[Jonathan de Boyne Pollard](#)
 - [Re: Timezones and appointments](#)
[Sean Smith Przemek Klosowski](#)
 - [Re: New Microsoft anti-piracy program circumvented](#)
[Peter Gregory](#)
 - [REVIEW: "File System Forensic Analysis", Brian Carrier](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Russian remote controlled submarine failure

<"Martyn Thomas" <martyn@thomas-associates.co.uk>>

Tue, 9 Aug 2005 15:00:12 +0100

A British Royal Navy remotely operated vehicle cut free the Russian submarine that was trapped 600 feet down. According to the British commander of the rescue, interviewed by BBC Radio 4 on 8 Aug 2005, the Russians had remote controlled vehicles of their own, but they failed because of a software error.

⚡ Caltrans screwup

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

Mon, 8 Aug 2005 15:58:55 PDT

Lauren Weinstein reported that Caltrans has started a 6-month experiment to put real-time travel times on freeway signs. The immediate result is apparently that traffic is tied up all over, as people slow down to read the signs!

⚡ Lightning causing problems for lightning-detection system

<Klaus Johannes Rusch <KlausRusch@atmedia.net>>

Wed, 03 Aug 2005 01:26:42 +0200

Fortunately there were only a few minor injuries when a plane overshot a runway at Pearson International Airport. According to a CBC report

(<http://www.cbc.ca/story/canada/national/2005/08/02/pearson-plane050802.html>)

most operations on the airport had been suspended due to bad weather: "... a spokesperson with the Greater Toronto Airports Authority said lightning was causing technical problems with the airport's lightning-detection system."

Why would one expect that lightning-detection systems could cope with lightning?

Klaus Johannes Rusch KlausRusch@atmedia.net <http://www.atmedia.net/KlausRusch/>

⚡ Lightning causing problems for lightning-detection system

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

Wed, 3 Aug 2005 14:59:40 PDT

My favorite meta-lightning event occurred was when I was giving a lecture in my Survivable Systems course at Maryland, and I was talking about the time at Wallops Island where they had several missiles ready to launch because they wanted to study the effects of lightning on the missile controls. As some of you may remember, lightning hit the launch platform and triggered the launching of one of the missiles (which I mentioned most recently in [RISKS-20.42](#)). Just at that point in the lecture, lightning hit the lecture room and took down the computer controlling the outfeeds to remote classrooms and our own video monitors. Some of the students wondered how I had managed such a theatrical effect.

⚡ Navy jet has severe brake failure

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

Fri, 5 Aug 2005 11:22:36 PDT

The F/A-18 Hornet has had a series of recent accidents many of which are being attributed to a very thin \$535 electrical cable that controls the

antiskid brakes. An investigation also concluded that cockpit procedures were confusing when pilots were confronted with brake failures. The U.S. military owns 561 Hornets, best known for their use by the Blue Angels.

[Source: AP report, 4 Aug 2005; PGN-ed]

http://www.rednova.com/news/general/197786/ap_navy_jet_has_severe_brake_problems/

⚡ US Navy to drop paper charts

<Scott Peterson <scott4@mindspring.com>>

Wed, 03 Aug 2005 00:51:24 -0700

Given some of the stories that have been posted here about the problems with electronic navigation systems, the mind boggles at the potential for disaster in this decision. [SP]

The U.S. Navy has committed to replacing its traditional paper nautical charts with advanced, interactive, electronic navigation systems throughout the fleet. The Electronic Chart Display and Information System - Navy is based on the voyage management system software programs developed by Northrop Grumman's Sperry Marine business unit, and operates with digital nautical charts -- a global database of digital charts produced by the National Geospatial Intelligence Agency. The Navy plans to equip the entire fleet of surface ships and submarines with Ecdis-N by the end of 2009, and no longer use paper charts after the electronic system is

certified.

[Source: Lloyds List, 2 Aug 2005; PGN-ed]

⚡ Re: US Navy to drop paper charts

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

Wed, 3 Aug 2005 14:55:04 PDT

Risks might occur when their Net connection is down and they cannot get their updated maps online! Remember the sub that ran into a rock. I wonder whether that rock has ever shown up on an online map since then?

⚡ Re: US Navy to drop paper charts ([RISKS-23.96](#))

<Scott Peterson <scottp4@mindspring.com>>

Wed, 03 Aug 2005 17:38:50 -0700

> I wonder whether that rock has ever shown up on an online map since then?

Actually part of the report on why that happened was because they were using the wrong paper charts and were not updating them properly. The correct charts did show a navigation hazard in that area.

<http://navysite.de/ssn/ssn711.htm>

On 9 May 2005, the Navy announced the completion of the investigation into the accident. The report states that "The findings of fact show that SAN

FRANCISCO, while transitting at flank (maximum) speed and submerged to 525 feet, hit a seamount that did not appear on the chart being used for navigation," and that "Other charts in SAN FRANCISCO's possession did, however, clearly display a navigation hazard in the vicinity of the grounding. SAN FRANCISCO's navigation team failed to review those charts adequately and transfer pertinent data to the chart being used for navigation, as relevant directives and the ship's own procedures required."

The report continues "If SAN FRANCISCO's leaders and watch teams had complied with requisite procedures and exercised prudent navigation practices, the grounding would most likely have been avoided. Even if not wholly avoided, however, the grounding would not have been as severe and loss of life may have been prevented."

⚡ Social Security Administration sends cards to the wrong place,

<Jonathan Kamens <jik@kamens.brookline.ma.us>>

Sun, 7 Aug 2005 22:30:35 -0400

won't admit it's due to buggy software they need to fix

The following is the introduction to

<http://www.mit.edu/~jik/ssa-zip.html>

-- which tells the whole story in sordid detail.

* * * * *

The software that the Social Security Administration (SSA) uses to

canonicalize mailing addresses when sending out social security cards has a bug which causes correct ZIP codes in some addresses to be replaced with incorrect ZIP codes.

This bug has been present for at least five years and has caused the social security cards for three of my children to be "lost" in the mail after their births.

The first two times this happened to me, the SSA resent a duplicate card when I contacted them and complained that the original had never arrived.

The first two times this happened to me, the SSA refused to investigate why the original card never arrived.

The third time this happened to me, I finally convinced the SSA to investigate, and the bug was exposed.

The SSA refuses to admit that the behavior of their software is a bug, despite the fact that any competent software engineer familiar with address-canonicalization technology would understand immediately that it is after being given a test case illustrating it.

The SSA refuses to issue a duplicate card for my youngest child unless I file a form SS-5, which requires that I either (a) send original, personal identification documents through the mail, which I am unwilling to do because of concerns about identity theft and document loss, or (b) submit the form SS-5 in person at one of their offices, which I am unwilling to do

because I think it's entirely unreasonable for me to have to miss work to correct the SSA's error.

The SSA has already admitted that my youngest child's card was lost in the mail and that they know why this happened. They've been corresponding with me at the address to which the card was supposed to have been sent, which is in their records, which means that they know for a fact that I am the father of the child whose card was lost and that I am legally allowed to receive a copy of the card. That they nevertheless refuse to issue a duplicate card has no legitimate justification and can be explained only as bureaucratic inertia or a stubborn refusal to admit fault.

* * * * *

If there is anyone reading this who works for or has connections at the SSA and who has the knowledge and experience to understand the bug I'm trying to get them to fix (I've yet to reach anyone at the SSA who has admitted to understanding it), please help!

German social services software drops changes

<Debora Weber-Wulff <D.Weber-Wulff@fhtw-berlin.de>>

Tue, 09 Aug 2005 12:23:38 +0200

<http://www.heise.de/newsticker/meldung/62595>

The online computer news service heise.de reports that an error

in the software system A2LL, which computes welfare and jobless subsidies as well as administering the system, has dropped over 100.000 changes that should have been reported to health insurance providers.

New registrants, people going off welfare, address changes and the like were registered with the system and then the changes were automatically rescinded.

The error cropped up after a new version of the software was installed on the central servers. [Perhaps they installed a test system by mistake that just pretends to accept changes? -dww]

The missed changes will not affect the insurance status of the people involved, but staff at the insurance companies must take care of all of the changes by hand.

Prof. Dr. Debora Weber-Wulff, FHTW Berlin, Internationale Medieninformatik
10313 Berlin +49-30-5019-2320 <http://www.f4.fhtw-berlin.de/people/weberwu/>

⚡ Hermann Chinery-Hesse and software in Ghana

<jhhaynes@earthlink.net>
Tue, 9 Aug 2005 13:58:34 -0500 (CDT)

There is an interesting article in the August 2005 issue of IEEE Spectrum on the above subject. Mr. Chinery-Hesse runs a very successful

software

business in Ghana. Some of the high points:

- * Software that is lean and efficient, so it runs well on old PCs such as

 - 386/486. These are affordable in Ghana.

- * Software design for robustness under third-world conditions.

For example,

 - frequent writes to disk to minimize work lost of the power goes off, as it

 - frequently does.

- * Rather extreme measures to protect proprietary software, such as updates

 - installed in personal visits by software company employees.

This to cope

 - with conditions in a country where any sense of ethics is practically

 - nonexistent.

- * Shunning of open source software, on the grounds that having the source

 - makes it too easy for unscrupulous users to modify the code so as to line

 - their own pockets.

This last item could well be criticized as security through obscurity.

Surely the incentives are there for users to make a considerable effort to

tamper with closed source proprietary software. One could argue that open

source software would be easier to audit for unauthorized modifications.

But then who audits the auditors? And how can they be sure that the code

actually running in the machine is accurately represented by the source code

they can see.

This suggests a larger research topic: how can we make computer systems that

are guaranteed to "work right" when they are to be installed in a den of

thieves? Seems like this has applicability to the problem of

electronic
voting systems in the U.S.

✶ Greeting answering machine! (R H Draney)

<msb@vex.net (Mark Brader)>

Mon, 8 Aug 2005 01:56:48 -0400 (EDT)

* From: R H Draney <dadoctah@spamcop.net>
* Newsgroups: alt.usage.english
* Subject: Re: greeting answering machine!
* Date: 6 Aug 2005 18:40:47 -0700
* Message-ID: <dd3oqv02rdc@drn.newsguy.com>

Tony Cooper filted:

> I am unconventional, though. Just yesterday I called a
doctor's office
> and told them they'd left a message on my machine that was
intended for
> someone else. Neither my (first) name nor number registered
with the
> person in the doctor's office that left a message that "my"
appointment
> had been canceled because the doctor would be out-of-town. I
thought it
> was the considerate thing to do.

My mother has been getting a series of calls from some lawyer's
office in
North Carolina, telling her (or rather someone whose name is
unintelligible
on the message) to call back at such-and-such a number...she's
tried calling
the number several times and they always start off by asking her
to punch in
her case number...as she has no case to number, the attempt to
straighten
out these people ends there, with (1) some lawyer's client

wondering why his
counsel hasn't called him, (2) the lawyer raising the penalty to
the next
level for failing to make contact, and (3) my mother getting
more and more
recorded messages....r

⚡ Every odd digit of number A, even digit of number B

<Dan Jacobson <jidanni@jidanni.org>>
Thu, 04 Aug 2005 07:55:26 +0800

The Taiwan telephone company has done it again. On their work
order
notification they only show every odd digit of the phone number
to be
serviced, 2*8*4*8*, and then for extra security, only every even
digit of
the contact number, *5*5*7*0. But if contact number == phone
number, all is
revealed, 25854780.

⚡ The risks of cell-phone auto-spellers

<"Schlake (William Colburn)" <schlake@nmt.edu>>
Thu, 4 Aug 2005 15:24:23 -0600

(my phone made me look like an idiot)

The first time I tried sending an SMS message on my new phone, I
was
horrified at what happened. Attempts to type in a word
generated huge
blocks of garbage text, beeping, and a refusal of the phone to

continue. I
was trying to do it the "old way", by hitting a key multiple
times to tell
which of the three letters I meant.

"That would make me happy." -> "8442809666885553062553304427
79991"

The space represents a pause in my typing to wait for it to
reset the letter
selector. The new phone has smart spelling, so I can type a
single number
for each word and it will magically spell the word I want. I
resisted, but
the lure of magic won me over, and now I can SMS faster with
many less key
strokes. I'm very happy with it almost all the time. Magic is
great stuff!

Today I sent an SMS message.

"That would make me happy." -> "8428096853062530630427791"

Except....

"8428096853062530630427791" -> "That would make if happy."

My cat is named "If", so now it suddenly looks like I'm talking
about my cat
(and I misspelled his name), and not me.

I immediately sent a followup message where I manually corrected
the
spelling of "me" and appended a second sentence: "I have to pay
more
attention to the auto speller."

The reply was: "You mean pay more attention."

First thought: Oh no, what I did I send? Thankfully, I only
sent "I must
pay more attention to the auto speller."

It is embarrassing that I made the same error in my message correcting myself. The risks are that magic isn't a DWIM. If the phone could 'do what I meant' then I could talk to my phone in plain english to transmit my message to someone halfway across the country[1], and not have to manually type my message into it. Another risk is complacency: I have grown to depend on auto-spelling, which is right so often that I've stopped reading what it is doing and I just continue merrily typing away assuming that everything is golden.

[1] I find it surprising how many people I know who consider their phone to be a text-messaging platform that happens to have voice-chat capabilities instead of a voice-chat platform that happens to have text-messaging capabilities.

✶ Credit-card obfuscation

<"Schlake (William Colburn)" <schlake@nmt.edu>>

Tue, 9 Aug 2005 10:24:29 -0600

I made a purchase from Bibliomania! today. I wasn't able to get the book I wanted through either amazon.com or ecookbooks.com, so I used the site suggested by the author of the book. I'm pretty mistrustful of online merchants, but this one had an SSL page for the credit card info and I really wanted the cookbook, so I went for it. The confirmation page that

came up, that it encouraged me to print, obfuscated my credit card number by "x"ing out the last four digits.

The risk is that the last four digits are normally the ones not "x"ed out by every other credit card processor that I've ever seen, so this confirmation plus any other confirmation gives you 20 digits of a 23 digit credit card number, and most places don't ask for the last 3 digits yet (card number YYYY YYYY YYYY YYYY expires yy/yy series zzz is 23 numbers).

Thankfully the unencrypted confirmation e-mail they sent didn't mention anything about the credit card at all, and it came in plain text and not HTML.

[Note: PGN changed occurrences of "x" to y and z, to avoid filtering.]

Re: Car computer systems at risk to viruses ([RISKS-23.96](#))

<Adam Laurie <adam.laurie@thebunker.net>>

Tue, 09 Aug 2005 11:19:13 +0100

Car kits are not only vulnerable to viruses, but also to privacy invasion through eavesdropping of audio via the telephony microphone, as well as social engineering attacks or simple 'nuisance calls' by pushing audio into the car speaker systems... The proof-of-concept tool "Car Whisperer" can be found here, along with more details of the attack:

http://trifinite.org/trifinite_stuff_carwhisperer.html

Adam Laurie, The Bunker Secure Hosting Ltd., Shepherds Building,
Rockley
Road, London W14 0DA UK <http://www.thebunker.net> +44 (0) 20
7605 7000

Re: Increasing sophistication of phishing spammers (Wallach, RISKS-23.60)

<Jonathan de Boyne Pollard <J.deBoynePollard@Tesco.NET>>

Wed, 15 Dec 2004 20:47:28 +0000

W> ... should pay attention to referrer information to refuse
images being

W> sent to pages other than their own.

Checking referrer headers at the content HTTP server is not
necessarily the
wisest course of action. It is easy to do wrongly, has
maintenance problems
for the publisher, and is conceptually shaky as well. And it
isn't
addressing the issue actually at hand, in any event. The far
better way to
address the issue at hand is one that many people have been
advocating for
quite some time now, for this and other reasons: ensure that all
MUAs are
designed *not to automatically fetch external content* when
displaying
messages (with body parts of any sort, not just "text/html",
moreover).

<URL:<http://homepages.tesco.net/~J.deBoynePollard/Proposals/gnksoa-mua.html#NoAutoFetchExternalContent>>

The RISK? Thinking that RFC 2017 is a good idea. (-:

I'm not aware of anything as detailed as the GNKSoA and the GNKSoA:MUA for web browsers and HTML display engines, but were there one, one of my suggestions for inclusion in it, that pertains here, would be the display of (CIS) URLs broken-down into their component pieces, preventing the confusion between domain parts and usernames that is often also exploited by these electronic mail scams.

W> Probably the only true answer is for eBay, my credit card company,

W> and all of these other vendors to start digitally signing their mail.

It is interesting to note how many of these same companies make a point of

noting that they provide end-to-end validation when one is accessing their

web sites (For the case of eBay, for example, see

<URL:http://pages.ebay.com./securitycenter/avoiding_fraud.html#secure>.),

and yet fail to do the same thing for their electronic mail communications.

However, one should always bear in mind that the architecture of SMTP-based

Internet electronic mail is the architecture of paper mail. The former is

simply, and solely, cheaper ("There are fewer electrons in an electronic

mail message than in a sheet of paper. So it's cheaper by weight."),

allowing the architectural flaws to be revealed more readily.

Digital

signatures **are** the tool for determining whether a message came from whom

it purports to have come from. However, look at paper mail and consider:

When you last received a paper communication from such a

company, was it on
mass-printed stationery with a computer-printed copy of
someone's signature
at the end? How did you know that that was the correct
signature? What
steps did you take to validate it? Do you even know what the
person's
correct signature is supposed to look like? When you next
contacted the
company, did you use the contact information (telephone number,
et al.)
supplied at the bottom of such a letter? When you telephoned
the company's
customer account line using the telephone number from the
letter, did you
supply your account number and password to the complete stranger
on the
other end of the line?

✉ **Re: Timezones and appointments (Rothwell, [RISKS-23.96](#))**

<Sean Smith <sws@cs.dartmouth.edu>>

Wed, 3 Aug 2005 19:22:52 -0400

I've had the inverse happen: a timer program that allows me to
turn my
laptop into an alarm clock insisted on working according to the
local time
back home in the US, rather than local time in the UK where I
was---even
though the system time zone had been changed to the UK.

Sean W. Smith, Ph.D. sws@cs.dartmouth.edu www.cs.dartmouth.edu/
~sws/

Department of Computer Science, Dartmouth College, Hanover NH USA

✉ **Re: Timezones and appointments (Rothwell, [RISKS-23.96](#))**

<przemek.klosowski <przemek.klosowski@gmail.com>>

Thu, 04 Aug 2005 22:36:27 -0400

I suspect that Mr. Rothwell stored the appointments for his US trip in US local time values, but didn't tell that to the computer. Consequently, the PDA assumed that he meant UK times, and shifted the values.

My left or your left? or rather, my 6 PM or your 6 PM? Most people would raise this issue when setting an appointment across time zones. What we need is a good user interface that allows, but doesn't always force us, to specify the time zone in which the event is being entered. Perhaps the UI should put up a time zone wizard if it matches "airport, flight, travel, etc." among proximate events.

✉ **Re: New Microsoft anti-piracy program circumvented ([RISKS-23.95](#))**

<Peter Gregory <petergregory@yahoo.com>>

Wed, 3 Aug 2005 12:25:54 -0700 (PDT)

In my opinion, the most amazing part is that Microsoft DOES NOT CONSIDER THIS TO BE A SECURITY FLAW. Will they respond in like manner when large numbers of cars fall victim to the first wide-spreading, car-infecting worm?

Peter Gregory, CISA, CISSP, Chief Security Strategist,
VantagePoint Security LLC, Bellevue, WA
phg@vantagepointsecurity.com

[Source: Hackers break into Microsoft's anti-piracy system.
PGN]

<http://www.techworld.com/security/news/index.cfm?NewsID=4134>

REVIEW: "File System Forensic Analysis", Brian Carrier

<Rob Slade <rslade@sprint.ca>>
Mon, 8 Aug 2005 08:09:38 -0800

BKFSFRAN.RVW 20050608

"File System Forensic Analysis", Brian Carrier, 2005, 0-321-
26817-2,

U\$49.99/C\$69.99

%A Brian Carrier

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8

%D 2005

%G 0-321-26817-2

%I Addison-Wesley Publishing Co.

%O U\$49.99/C\$69.99 416-447-5101 800-822-6339 bkexpress@aw.com

%O <http://www.amazon.com/exec/obidos/ASIN/0321268172/>

[robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0321268172/robsladesinterne)

<http://www.amazon.co.uk/exec/obidos/ASIN/0321268172/>

[robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0321268172/robsladesinte-21)

%O <http://www.amazon.ca/exec/obidos/ASIN/0321268172/>

[robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0321268172/robsladesin03-20)

%O Audience a- Tech 2 Writing 1 (see revfaq.htm for
explanation)

%P 569 p.

%T "File System Forensic Analysis"

The preface states, correctly, that there is little information
for

the forensic investigator on the topic of file system structures and internals that are useful for providing direction on tracing and tracking information on the disk. The author also notes that there are a number of worthwhile texts that address the general topic of investigation. Therefore, the author intends to address the former rather than the latter. At the same time, there is an implication in the initial section that this work is only the merest introduction to the subject of computer forensics.

Part one is aimed at providing foundational concepts. Chapter one, in fact, does provide a quick review of the investigation process, and a list of forensic software toolkits. A sort of "Computers 101" is in chapter two, with a not-terribly-well structured collection of facts about data organization, drive types, and so forth, with varying levels of detail. Chapter three addresses different factors and problems in hard disk data acquisition, although the inventory is neither complete nor fully explained.

Part two deals with the analysis of drive volumes or partitions, with chapter four outlining basic structures. DOS (FAT [File Allocation Table] and NTFS) and Apple partition details are discussed in chapter five. Chapter six reviews various UNIX partitions. Multi-disk systems, such as RAID (Redundant Array of Inexpensive Disks) are covered in chapter seven.

Part three delves into the data structures of the file system itself. Chapter eight introduces concepts used in considering file systems. Details of the FAT system are in chapters nine and ten. A very detailed

explanation

of the disk and file structures of the NTFS system, as well as considerations for analysis, is provided in chapters eleven to thirteen.

The Linux Ext2 and Ext3 structures are discussed in chapters fourteen and fifteen. Chapters sixteen and seventeen cover the UFS1 and UFS2 schemes, found primarily in BSD (Berkeley Systems Distribution) derived versions.

This book does provide a wealth of detail, once it gets into the specifics of partitions and structures. The introductory material, writing, and technical level are quite uneven, which makes it difficult to use. Still, those seriously involved with the data recovery aspect of digital forensics should consider this work a valuable resource.

copyright Robert M. Slade, 2005 BKFSFRAN.RVW 20050608
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.
niu.edu
http://victoria.tc.ca/techrev or <http://sun.soci.niu.edu/~rslade>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 2

Sunday 28 August 2005

Contents

- [The Time Has Come: Taking Our Issues to the Public](#)
[PGN](#)
- [Customs Computers Fail](#)
[Chuck Weinstock](#)
- [10th "planet" discoverer shares a secret a bit earlier than planned](#)
[George Swan](#)
- [Hospital struck by computer virus](#)
[Andrew Brydon](#)
- [USAF personnel database compromised](#)
[Ross Stapleton-Gray via Dave Farber](#)
- [Students face punishment for computer tampering](#)
[Thom Kuhn](#)
- [Cellphone carriers can listen in through your phone](#)
[Ryan Block via Dave Farber](#)
- [No inspection record, lack of human contact, or something else?](#)
[Mythdraug](#)
- [Risks of First UTC Leap Second in 7 Years](#)
[Dave Glicksberg](#)

- [Teacher concerns over L.A. school computerization project](#)
[Lauren Weinstein](#)
 - [Re: Navy jet has severe brake failure](#)
[Carl F](#)
 - [Bad password practices](#)
[Jeremy Epstein](#)
 - [Risks of Bluetooth pirates?](#)
[Andre Kramer](#)
 - [Re: Risks of REAL ID: incorrect](#)
[Charles P. Lamb](#)
 - [Re: US Navy to drop paper charts](#)
[R A Lichtensteiger](#)
 - [Re: Slade's review of "File System Forensic Analysis", Brian Carrier](#)
[Simson Garfinkel](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ The Time Has Come: Taking Our Issues to the Public

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

Sun, 28 Aug 2005 19:29:42 PDT

My note in [RISKS-23.96](#) on 20 years of putting out issues of the ACM

Risks Forum has led me to reflect further on what we have accomplished in the way of progress and what remains to be done.

The basic problems considered here keep recurring. Whatever progress might be made in computer-related technologies and their applications has not been reducing the threats, vulnerabilities, and risks related to the systems upon which we individually and as a civilization depend most. Overall, this leads me to a sense of frustration that the Risks

Forum has been largely preaching to the choir, and that our message is not getting through to those who really need it most. All of you regular RISKS readers are likely to be totally unsurprised by the items that you read here --- they are just more of the same. Occasionally we might gain a new convert in the understanding of the depth of problems of what is wrong and what is needed to meaningfully address those problems.

Somehow we need to be able to reach out professionally and effectively beyond the RISKS audience. I have testified at least a dozen times for governmental bodies on RISKS-related issues, but always have a gnawing feeling that these efforts fall on deaf ears or are largely ignored by brains that are preoccupied with other concerns.

There are quite a few of you in the academic community who have consistently represented the best principles that might be gleaned from the RISKS experiences, such as Peter Denning, Rebecca Mercuri, Dave Parnas, and Jerry Saltzer, to name just a few. There are also quite a few of you working for commercial companies who have done the same, such as Jim Horning.

There are also a few organizations that are able to gather dedicated people and financial resources to keep pressures up on certain aspects of the RISKS problems -- for example, EPIC, EFF, and CDT on the legal issues relating to privacy and human rights.

Beyond that, there are just a few of our RISKS readers who operate essentially on a pro-bono basis with effectively no funding at

all.

Notable among these is Lauren Weinstein, who as many of you know has been a very long-time contributor to RISKS and a wide variety of other venues, and the most prolific guest columnist for my CACM Inside Risks series. Because he has no ongoing institutional support, his continuing time spent and efforts in these areas have been decidedly to his own financial detriment, to the extent that merely keeping the lights on is literally an issue for him these days.

Despite this circumstance, he has been strongly advocating a new outreach project that I believe could be very important not only toward making genuine progress in RISKS-related matters but in other areas of concern as well.

He believes -- and I do too -- that those of us who worry about risks, hype, propaganda, distortions, and the general demise of scientific and realistic thinking have been outflanked by well-funded, vested interests who have everything to gain from maintaining the status quo. Further, making real progress against such entrenched forces means moving outside of the confines of preaching-to-the-choir Internet mailing lists and Web sites.

When we can occasionally create sensible public discussions of hype-free facts about technological risks, effects of technology on society, privacy, security, and many other related topics, the response is generally enthusiastic and usually not politically biased.

Most often we hear, "Why has nobody told us about this before!"

We both agree that a significant nonpolitical, media-based outreach

may represent the best hope of making some real progress, by directly reaching the vast audiences who all too often have been misled about what's really going on.

Few of these persons can be expected to subscribe to RISKS or other such forums, especially because they are unlikely to even realize that many of these problems exist. Thus, it is necessary to go to the commercial broadcast media from which most people get their information and misinformation. Commercial radio is clearly a key medium to this end, whereas public broadcasters such as National Public Radio generally have very limited program schedules and do not reach the full spectrum of listeners of concern.

The essence of Lauren's project idea is to achieve a significant outreach push into commercial radio, with the aim being to provide various forms of programming that would ``tell it like it is'' but not be politically biased yell-fests. Lauren has the necessary on-air broadcasting and production experience (many of you have heard his various commentaries and other works over the years), and the required technical abilities.

I feel that this is an excellent approach and would be very valuable, but Lauren simply cannot move forward along these lines unless there is some source of significant funding -- advertisers, underwriters, "angels", or other interested parties -- to seed and keep the project going long enough to build a following among stations and listeners.

Lauren takes pains to point out that this would be a significant effort that would require a considerable period of time, and that there's no guarantee of success. I feel that it would be well worth the effort for him to forge ahead with this (or related efforts that would usefully move these issues forward), if suitable funding can be found.

Please let Lauren (lauren@vortex.com) and me (neumann@csl.sri.com) know if you, or other organizations or entities, might be interested in helping to make this happen. Thank you. PGN

✈ Customs Computers Fail

<Chuck Weinstock <weinstock@conjelco.com>>
Fri, 19 Aug 2005 15:47:23 -0400

A U.S. Customs database system in Virginia shut down for about 5.5 hours beginning around 6pm on 18 August. The system is used to process incoming international air passengers, but its absence caused havoc at Miami International Airport, where up to 2000 people were waiting to clear immigration. Airports in the NYC area were able to use backup systems.

[The cause was subsequently blamed on a virus, according to Lisa Orkin Emmanuel, Associated Press/AP Online, 22 Aug 2005; PGN-ed]

⚡ 10th "planet" discoverer shares a secret a bit earlier than planned

<George Swan <geoswan@primus.ca>>

Tue, 23 Aug 2005 17:52:06 -0400

Planetary Astronomer Michael Brown, one of the co-discoverers of various Kuiper Belt Objects, including Sedna, the really distant one, recently announced the discovery of a Kuiper Belt Object even larger than Pluto.

His web-page indicates why he released the information about the discovery earlier than planned:

<http://www.gps.caltech.edu/~mbrown/planetlila/#discovery>

He became concerned late in July, after he had learned that the computers that controlled the telescopes his team used for their observations kept publicly searchable logs of where the telescopes had been pointed. (From his description it sounds to me as if these logs must also contain a code for what they were looking at.) Brown also realized that they had used some of their codenames in the publicly available abstracts for some upcoming talks. A call to the Minor Planet Centre revealed that someone had recently used a tool the MPC provides to plot the location of his team's tenth planet for that very night! A hurried press conference followed.

⚡ Hospital struck by computer virus

<Andrew Brydon <andrew@isbjorn.demon.co.uk>>

Mon, 22 Aug 2005 19:44:18 +0100

Up to 300 radiotherapy patients were turned away from a hospital in Bebington, Merseyside, UK, after a computer virus infected equipment.

<http://news.bbc.co.uk/1/hi/england/merseyside/4174204.stm>

⚡ **USAF personnel database compromised (From Dave Farber's IP list)**

<Ross Stapleton-Gray <ross@stapleton-gray.com>>

August 22, 2005 2:22:34 AM EDT

Using an airman's log-in information to access the online Assignment Management System (AMS) and download data from it, someone gained access into an Air Force personnel system and accessed individual information on about half of its officers and "a handful" of its noncommissioned officers. The Air Force has started notifying more than 33,000 service personnel of the security breach, according to a statement. ... Air Force officers can log in at www.afpc.randolph.af.mil/vs to see if their information was compromised. The service will call the enlisted members whose information the hackers viewed. [Source: Hacker nabs Air Force personnel data, Frank Tiboni, *Federal Computer Week*, 19 Aug 2005]
<http://www.fcw.com/article90229-08-19-05-Web>

★ Students face punishment for computer tampering

<"Thom Kuhn" <tkuhn@mail.acponline.org>>

Wed, 10 Aug 2005 20:08:32 -0400

Thirteen high-school students in the Kutztown Area School District (Pennsylvania) face felony charges of tampering with computers after defeating security measures on laptops issued to them by the school district. They used administrator passwords (taped to the backs of the computers) to override Internet filters and download software such as iChat that the district policy forbids. The laptops included an application that allowed district administrators to see what students did with the computers. However, the students modified the monitoring program so that they could see what the administrators did with their computers. The students and their parents argued that the felony charges are unwarranted, but, according to the district, students and parents signed acceptable use policies that clearly state what activities are not allowed and that warn of legal consequences if the policy is violated. The students continued to violate district policies for use of the computers even after detentions, suspensions, and other punishments, according to the district. Only then did school officials contact the police. [*Wired News*, 9 August 2005; PGN-ed]

<http://www.wired.com/news/technology/0,1282,68480,00.html>

⚡ Cellphone carriers can listen in through your phone, Ryan Block

<David Farber <dave@farber.net>>

Fri, 5 Aug 2005 11:09:55 -0400

Ryan Block, Cellphone carriers can listen in through your phone,
Aug 5, 2005,

<http://cellphones.engadget.com/entry/1234000563053276/>

We're always a little wary of that very blurry line between protection of the general public and infringements on basic civil liberties, but it would appear that according to the Financial Times by way of the Guardian, at least one UK cellphone carrier not only has the power (and mandate) to remotely install software over the air to users' handsets that would allow for the kind of monitoring we thought only perverts and paranoiacs had access to: picking up audio from the phone's mic when the device isn't on a call. While don't think the backlash on this one has really gotten underway yet, and though we do hate to rock a cliché', we can't help but be reminded of that classic Benjamin Franklin quote, ``They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.''

What's worse, a cellphone carrier and The Man are gonna take it from us without our permission on the sly?

⚡ No inspection record, lack of human contact, or something else?

<"Mythdraug ." <mythdraug@gmail.com>>

Thu, 11 Aug 2005 12:05:49 -0500

First some background.

I have signed up with my local gas company (Peoples Gas) for online payment and billing. As part of the process they, of course, require my e-mail address. In late May I received a postal letter informing me of their need to perform an inspection of my inside lines under threat of being disconnected if we failed to comply. Naturally, I scheduled an appointment. A technician came and mechanically sniffed the joints in the line said thanks and walked out the door.

Fast forward to a much more recent day. Via the e-mail address which I signed up for online service with them, I receive a letter admonishing me for failing to allow the mandatory inspection. I was again threatened with disconnection for failure to comply.

Knowing that I had previously had the inspection completed, I replied to the message stating exactly that. The e-mail bounced from their system as undeliverable. I called the phone number provided in the message, only to be connected to an automated system for setting an appointment with no obvious way to reach an operator.

At this point, you may think that my complaint is in not being presented with an audit record at the time of inspection. Or perhaps, I am frustrated that there was no clearly defined way to break out of the process or way for me to indicate that my inspection had already

been performed.

You would be incorrect. You see, what I haven't yet mentioned is that they had addressed that message to me by placing my e-mail address on the CC line. But it wasn't just my e-mail address there, it was the e-mail address of everyone (well I guess only half of them actually as the list began with purplerose3637@*****.net; PWOODWARD1966@*****.com and ended with zedwards@***.com; zoldowski@*****.net) receiving the notification. Yes, that is correct, I now have the e-mail address for ~240 people who are in risk of having their gas disconnected.

The privacy policy on their web site (<http://pecorp.com>) states "We will never willfully sell, trade, rent, disclose, or make available personally identifiable information to any third party without first receiving your permission, except when we believe in good faith that the law requires it, or to protect the rights or property of Peoples Energy."

The risks? I'll let you decide....

⚡ Risks of First UTC Leap Second in 7 Years

<Dave Glicksberg <davidg@bourbaki.jpl.nasa.gov>>
Mon, 22 Aug 2005 18:58:22 -0700 (PDT)

[Originally submitted 2005-07-07, but lost in the shuffle.
PGN]

The International Earth Rotation Service (IERS, <http://www.iers.org>) just announced a UTC leap second for the end of 2005, specifically at 2005-12-31T23:59:60Z (see <http://hpiers.obspm.fr/eoppc/bul/bulc/bulletinc.dat>).

The previous leap second was 7 years before, at 1998-12-31T23:59:60Z, which was before Y2K! In contrast, from UTC's inception in 1972 through 1998, leap seconds were fairly common, occurring every 0.5 to 2.5 years.

UTC is the basis for civil and military timekeeping worldwide. It is transmitted in coded radio time signals like WWV, and it is used by Russia's navigation satellites GLONASS (<http://www.glonass-center.ru/stime.html>), which therefore must accommodate leap seconds. However, GPS satellites use a continuous timescale that does NOT have leap seconds.

THE RISKS?

* In the 7 years since the last leap second, maintainers of systems and software that are UTC-aware may have forgotten how to properly handle a leap second, whether it is done manually or automatically (e. g. by synchronization with WWV, or with time servers that properly handle the leap second).

* Newer systems and software have never encountered a leap second, unless via thorough testing. Some systems may have omitted consideration of leap seconds altogether!

* Potential downtime or errors due to the need to do a manual update, or due

to incorrect automatic updating.

* Consequences of forgetting that the leap second occurs simultaneously around the world, regardless of local time zone. In New York, the leap second will occur at 7PM (actually, 18:59:60) on New Year's eve, and in Moscow, it will occur at 3AM (02:59:60) New Year's Day.

Dave Glicksberg -- glicksbergd AT eh see em DOT oh are gee -- MY OPINIONS ONLY

✶ Teacher concerns over L.A. school computerization project

<Lauren Weinstein <lauren@vortex.com>>

Sat, 27 Aug 2005 10:14:32 -0700

A friend of mine here in L.A. -- a middle school teacher in the Los Angeles Unified School District for around 30 years -- sent me the note below.

LAUSD is the second largest school district in the country, and is embarking on a computerization project that has many teachers concerned. The driving force appears to be the desire to obtain every last possible attendance dollar per student, despite the risks that appear obvious even to persons who are not computer experts.

- - - -

Thought you would want to hear about the latest L.A. school district new program for attendance taking and report card grades. It rolled out earlier this year at some schools already and should be debuting soon at

many

secondary schools by October. Every teacher has been mandated to set up an LAUSD e-pal account so that we can now do on-line attendance taking and grades. We were promised to have an additional brand new computer installed in our classrooms over the summer. All rooms were wired prior to summer vacation. Next semester we are being asked to take and report by computer attendance for every single class in real time, period by period, by logging into our e-mail account and using our issued password. Many teachers are a bit nervous about adjusting to the new requirement and the time away from focusing on instruction. We were warned to protect our password as if our career depended on it, keeping in mind what an evil-minded child could do on the system if our password got into their hands.

The whole program originally named ISIS (after an Egyptian goddess) was just changed to LAUSDMAX. Their hope is that time and paper will be saved. I am a bit nervous about having to run to my attendance computer multiple times a day, especially when my school like most others can have multiple tardy students during a typical period which would require attendance adjustments for accuracy. I hope the district knows what it is doing and is not backing itself into another financial disaster. Can you imagine the problems substitute teachers will face? You would think they would be smart and just ask us to do the attendance in just one sitting at the end of the school day. Teachers are waiting to see if they make us maintain a paper rollbook

as well. Will we be doing more or less work?

✉ **Re: Navy jet has severe brake failure ([RISKS-24.01](#))**

<<carlf@panix.com>>

Wed, 10 Aug 2005 17:10:52 -0400 (EDT)

> The F/A-18 Hornet has had a series of recent accidents many of
> which are
> being attributed to a very thin \$535 electrical cable that
> controls the
> antiskid brakes ...

Where "recent" dates back to 1990? There may well be a problem,
but 24
accidents in 15 years is hardly "a series of recent accidents".

As the Navy spokesperson said, every significant accident
involved failures
by the pilots to follow procedure (notably one pilot not knowing
how to use
the emergency brakes!).

I don't know that this is a Risk In Computing.

[REMINDER: Risks in the Use of Computers are often interface
problems,
educational problems, training, experience, etc. PGN]

✉ **Bad password practices**

<Jeremy Epstein <jeremy.epstein@cox.net>>

Wed, 10 Aug 2005 14:12:18 -0400

I recently applied for and got an account on a moderately sensitive government computer system that's accessed over the Net. You apply by sending various information (such as name & address, but not SSN) to them by e-mail. A person then reviews the request, and sends you back the account information.

Two interesting things:

1. When my account was issued, the username and password were sent in two separate e-mail messages. That's a good practice (certainly not foolproof, but better than sending in one message). However, they were sent just seconds apart from the same address and to the same recipient address, which dramatically reduces the value of separating them. Doubtless, someone said "it's dangerous to send them together", but didn't consider that sending the impact of sending them at the same time.

2. The password is a fairly high quality value (seven random-looking letters and numbers, but no special characters). However, it's not changeable.

So, my sensitive password came via e-mail, most likely will get written down, and can't be changed. Now *that's* a secure system!

⚡ Risks of Bluetooth pirates?

<"Andre Kramer" <andre.kramer@eu.citrix.com>>
Thu, 18 Aug 2005 11:31:28 +0100

The Cambridge Evening News reported yesterday ("Phone Pirates in seek and steal mission" 17th August 2005) that several laptop computers have been stolen from car boots (automobile trunks for US readers) in Cambridge (UK). The article claimed that "Bluetooth" was used to detect the laptops presence. While the thefts appear related, the claimed modus operandi seems unlikely as short range wireless would be inactive unless the laptops were powered on (to be fair, the article also mentioned "other electronics"). The risk: thinking your devices are safe in the car boot when they don't have wireless.

✉ **Re: Risks of REAL ID: incorrect (Re: [RISKS-23.95](#))**

<"Charles P. Lamb" <clamb@acm.org>>

Wed, 10 Aug 2005 16:58:42 -0400

The article from [RISKS-23.95](#) with subject Risks of REAL ID and the linked **The Boston Globe*/Associated Press* article are incorrect. The REAL ID Act doesn't require states to do anything. The law states only requirements for use of a state-issued driver's license, or any other identification card, as a Federal ID. In the words of the law itself:

"(1) IN GENERAL. Beginning 3 years after the date of the enactment of this division, a Federal agency may not accept, for any official purpose,

a driver's license or identification card issued by a State to any person

unless the State is meeting the requirements of this section."

If a state intends its driver's licenses to be used **only** as driver's licenses, it need do nothing.

[This could lead to some curious results. If every state were to claim

that its licenses are to be used only as licenses, then all state elected

officials could not use their drivers' licenses to board commercial

aircraft. Or the Feds might just say that those state licenses must be

considered as de facto Federal IDs (whether or not they actually satisfy

the requirements). PGN]

✉ Re: US Navy to drop paper charts (Scott Peterson, PGN, Scott Peterson)

<R A Lichtensteiger <rali@Tifosi.com>>

Sun, 14 Aug 2005 00:44:36 -0400

Scott Peterson <scottp4@mindspring.com> wrote (in [Risks 24.01](#))

<> Given some of the stories that have been posted here about the problems with

<> electronic navigation systems, the mind boggles at the potential for

<> disaster in this decision. [SP]

The biggest problem is the same one that applies to paper charts and

modern navigation technologies. GPS shows you where you are on the

planet's surface, not where you are on the chart. Cross up your datums and things are just as apt to go "bump" in the night ...

Once again, the mediation is the same melody: "Never place all of your trust in a single system" whether that system is GPS, ECDIS or a lightning detector.

So long as running into things continues to be a "career limiting move" for the commanding officer, I suspect the Navy will continue to be very good about cross checking what different navigation inputs claim for the ship's position.

For commercial shipping, with it's much smaller crews, and civilian sailors, the level of faith placed in a GPS and chartplotter scares me.

Peter G. Neumann <neumann@csl.sri.com> added (in the same Risks digest):

<> Risks might occur when their Net connection is down and they cannot get
<> their updated maps online! Remember the sub that ran into a rock. I wonder
<> whether that rock has ever shown up on an online map since then?

Charts are updated with a system of "Notices to Mariners" and "Local Notices To Mariners." They are published on a weekly or monthly basis, available electronically, or by snail mail. With paper charts, the information then needs to be (accurately!) transcribed onto the chart. Given this time lag, one's net connection would have to be pretty solidly down for ECDIS-N to not be an improvement on the older system.

(Not that
I put that beyond the USN's capability, mind ...[1])

[1] Snotty remark from a former USCG navigator!

[Later note:

You might find the USCG's E-Nav website interesting (or
some of
your readers may):

<http://www.navcen.uscg.gov/enav/default.htm>

]

✉ Re: Slade's review of "File System Forensic Analysis", Brian Carrier

<Simson Garfinkel <simsong@eecs.harvard.edu>>

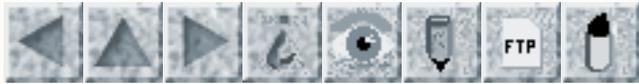
Fri, 12 Aug 2005 21:20:31 +1200

I need to take issue with Rob Slade's review of Brian Carrier's new book.

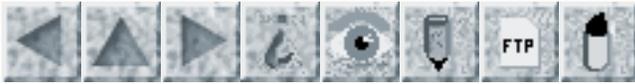
File System Forensic Analysis is really an excellent book. It not only is the first to go into the topic, but it has so much detail that it is likely to be of invaluable assistance to both practitioners and researchers for many years to come.

I am completely baffled by Slade's criticism of the book taking a while to get to technical details, and his complaint that the book is uneven. Brian's book is specifically designed to be approachable to both a person who is new to the field and a seasoned expert. it does a great job with this goal.

Indeed, if there was no introductory material, I imagine that Slade would have criticized File System Forensic Analysis for being impenetrable or unusable for people new to the field.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 3

Weds 7 September 2005

Contents

- [Katrina's telecom damage tops \\$400 Million; repairs may take months](#)
[Monty Solomon](#)
- [Cockpit confusion found in Cypriot airliner crash](#)
[Lindsay Marshall](#)
- [Flight Control System Software Anomalies](#)
[Peter B. Ladkin](#)
- [Ships relying on GPS-based systems](#)
[Peter B. Ladkin](#)
- [VT Gas pumps give up at \\$3/gallon](#)
[Monty Solomon](#)
- [UK Elections: Web and text vote trials dropped](#)
[Chris Leeson](#)
- [German social services software with new, costly errors](#)
[Debora Weber-Wulff](#)
- [Not guilty because of system deficiencies](#)
[Debora Weber-Wulff](#)
- [The FBI Virtual Case File and other disasters](#)
[jhhaynes](#)

● [Mercedes car-door locking functionality](#)

[Leon Kuunders](#)

● [Re: Risks of Bluetooth pirates?](#)

[Vassilis Prevelakis](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ Katrina's telecom damage tops \$400 Million; repairs may take months

<Monty Solomon <monty@roscom.com>>

Tue, 6 Sep 2005 22:49:42 -0400

BellSouth reports that the telecom damages from Hurricane Katrina in the New Orleans/Mississippi Gulf Coast area are on the order of half a billion dollars, with repairs taking 4 to 6 months, according to preliminary estimates. Roughly 1.1 million lines are still out. [Source: Arshad Mohammed, *The Washington Post*, 6 Sep 2005; PGN-ed]
<http://www.washingtonpost.com/wp-dyn/content/article/2005/09/05/AR2005090501231.html>

[Of course, those costs are dwarfed by the overall catastrophe. The huge magnitude of the natural disaster, the lack of foresight over past decades in protecting the levees, and the many problems with emergency responses are horrendous. This once again reminds us of the extent to which we tend to deprecate far-sighted proactive risk management. PGN]

⚡ Cockpit confusion found in Cypriot airliner crash

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

Wed, 7 Sep 2005 16:46:06 +0100

The crew members of a Cypriot airliner that crashed Aug 14 near Athens became confused by a series of alarms as the plane climbed, failing to recognize that the cabin was not pressurizing until they grew mentally disoriented because of lack of oxygen and lost consciousness, according to several people connected with the investigation into the crash. In addition, the German pilot and the young/inexperienced Cypriot co-pilot did not have a common language in which they could speak fluently, and had difficulty understanding each other's standard airline English. A total of 121 people were killed in the crash after the plane climbed and flew on autopilot, circling near Athens until one engine stopped running because of a lack of fuel. The sudden imbalance of power, with only one engine operating, caused the autopilot to disengage and the plane to begin to fall.

[Source: Don Phillips, International Herald Tribune, 7 Sep 2005; PGN-ed]

<http://www.nytimes.com/2005/09/07/international/europe/07cypriot.html>

[Also noted by Chuck Weinstock]

✶ Flight Control System Software Anomalies

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>

Wed, 31 Aug 2005 11:19:04 +0200

In this era of fly-by-wire, I am fond of saying that, as far as I know, there has never been a commercial aircraft accident caused by anomalies in flight control software. And it has been 17 years (the first A320 was introduced into service in 1988).

It is thus well to remember that designing and writing critical software-based systems for such applications is not a routine task that we now know how to perform. In fact, there are plenty of anomalies that crop up that the public doesn't hear about. Here is one that made it out, and a pointer to another.

The B777 is a high-capacity Boeing electric airplane (that is, fly-and-a-lot-of-other-things-by-wire) designed inter alia for intercontinental travel. The aircraft has been in service since 1995, and 490 of them have been delivered (for comparison, of Boeing's "jumbo", there are 625 B747-400 delivered, and a further 477 "classic" B747 still in service) [1].

The B777 has just been subjected to an emergency Airworthiness Directive (AD) from the U.S. FAA [2]. In April 2005, the FAA issued AD 2005-10-03 requiring "modification of the operational program software (OPS) of the air data inertial reference unit (ADIRU) from software version part number (P/N) 3470-HNC-100-03 to software version P/N 3475-HNC-100-06 or 3474-HNC-100-07. That AD resulted from a report of the display of erroneous heading information to the pilot due to a defect in the OPS of the ADIRU."

An AD is issued in response to an identified hazard, and the reasons are given as a list of possible consequences of the hazard, including worst-case consequences: "We issued that AD to prevent the display of erroneous heading information to the pilot, which could result in loss of the main sources of attitude data, consequent high pilot workload, and subsequent deviation from the intended flight path."

Attitude data consist of angle of pitch (nose up or down), angle of bank (left/right wing low/high) and heading. The flight control system, and pilots, also use the rate of change of these quantities, as well as their accelerations, although these are not presented as separate displays to pilots (one notes these are "trends" through cognitive processing rather than display).

Emergency AD 2005-18-51 was issued on August 29, 2005. An unsafe condition had been identified through analysis of an incident, and Boeing had issued an Alert Service Bulletin on August 26 addressing the problem with workarounds. The Emergency AD makes these actions mandatory. The FAA explains as follows:

Since [AD 2005-10-03] was issued, we received a recent report of a significant nose-up pitch event on a Boeing Model 777-200 series airplane while climbing through 36,000 feet altitude. The flight crew disconnected the autopilot and stabilized the airplane, during which time the airplane climbed above 41,000 feet, decelerated to a minimum speed of

158 knots,

and activated the stick shaker. A review of the flight data recorder shows

there were abrupt and persistent errors in the outputs of the ADIRU. These

errors were caused by the OPS using data from faulted (failed) sensors.

This problem exists in all software versions after P/N 3470-HNC-100-03,

beginning with P/N 3477-HNC-100-04 approved in 1998 and including the

versions mandated by AD 2005-10-03. While these versions have been

installed on many airplanes before we issued AD 2005-10-03, they had not

caused an incident until recently, and the problem was therefore unknown

until then. OPS using data from faulted sensors, if not corrected, could

result in anomalies of the fly-by-wire primary flight control, autopilot,

auto-throttle, pilot display, and auto-brake systems, which could result

in high pilot workload, deviation from the intended flight path, and

possible loss of control of the airplane.

We have evaluated all pertinent information and identified an unsafe

condition that is likely to exist or develop on other Boeing Model 777

airplanes of this same type design. Therefore, we are issuing this AD to

prevent the OPS from using data from faulted (failed) sensors, which could

result in anomalies of the fly-by-wire primary flight control, autopilot,

auto-throttle, pilot display, and auto-brake systems. These anomalies

could result in high pilot workload, deviation from the intended flight

path, and possible loss of control of the airplane. This new AD supersedes

AD 2005-10-03.

Note that the consequences list has been extended by "possible loss of control of the airplane". According to John Sampson, the incident to which the AD refers occurred to a Malaysian Airlines B777-200 on 3 August 2005, on Flight MH 124 from Perth to Kuala Lumpur [3]. The aircraft returned to Perth after 51 minutes flight for an emergency landing after an ADIRU malfunction which caused a "flight control outage".

This is the first public statement of which I know which addresses classes of Byzantine faults. Byzantine faults have occurred, seriously, in avionics before but the details are not public (see the quote from [6] below). Byzantine faults are faults in which agents (sensors, computers) in a distributed system "lie" to their interlocutors: they do not fail silently but distribute erroneous data, or data which is read differently by different receivers. The name arose from a whimsical analogy by Lamport, Shostak and Pease to a group of Byzantine generals trying to reach agreement in a situation in which no one trusts anyone else to speak the truth. The classic papers from twenty years ago are [4,5], and I understand arose from SRI International's involvement in trying formally to verify the operating system of the first digital flight control computer, SIFT.

Dealing with Byzantine faults became an extremely active area of distributed computing theory, but practitioners did not take them so seriously at first, perhaps partially due to the very high resource consumption of

the solutions: Lamport, Shostak and Pease showed that any correct algorithm to achieve consensus required a large number of processors (roughly speaking, at least $3n+1$, where n is the number of "liars") and a lot of processor cycles. It follows that solutions judged to be practical are unlikely to be complete solutions, and therefore one must analyse the actual problem space more closely to find out where one can most profitably handle possible problems, and which areas one can ignore.

The SAFEbus, the backplane communications bus of the B777 flight control system, now standardised as ARINC 659, was designed by Ken Hoyme and Kevin Driscoll at Honeywell. Driscoll, with Honeywell colleagues Hall and Zumsteg, and Sivencrona (Chalmers Uni, Sweden) wrote a paper in SAFECOMP 2003 in which they described occurrences of Byzantine faults in avionics and how one can deal with them (or not, as the case may be) [6]. They say "Byzantine faults in safety-critical systems are real and occur with failure rates far more frequently than $10^{(-9)}$ faults per operational hour. In addition, the very nature of Byzantine faults allows them to propagate through traditional fault containment zones, thereby invalidating system architectural assumptions."

Driscoll et al. refer to a set of incidents in which the occurrence of Byzantine failures "threatened to ground all of one type of aircraft". This set of incidents is not publicly available. I quote:

This aircraft had a massively redundant system (theoretically, enough redundancy to tolerate at least two Byzantine faults). but, no amount of redundancy can succeed in the event of a Byzantine fault unless the system has been designed specifically to tolerate these faults. In this case, each Byzantine fault occurrence caused the simultaneous failure of two or three "independent" units. The calculated probability of two or three simultaneous random hardware failures in the reporting period was $5 \times 10^{(-13)}$ and $6 \times 10^{(-23)}$ respectively. After several of these incidents, it was clear that these were not multiple random failures, but a systematic problem. The fleet was just a few days away from being grounded, when a fix was identified that could be implemented fast enough to prevent idling a large number of expensive aircraft.

The significance of the $10^{(-9)}$ figure is that airworthiness requires that a "catastrophic" failure of aircraft systems occur with a rate less than this per operational hour. The figure was originally chosen to be low enough that one would not expect a catastrophic failure during the lifetime of the fleet of that type aircraft (whether this calculation still holds is a separate question) [7]. Any hazard (for example, failure) with potentially catastrophic consequences which is seen or judged to have more frequent occurrence can lead to withdrawal of the airworthiness certificate of the type. Hence Driscoll et al.'s story.

I do not know (yet) whether the fault identified in AD 2005-18-

51 is of one
of the types specifically considered by Driscoll et al.

Circumstances in which messages are sent which are misinterpreted by receivers are not at all unusual. It is not clear that Driscoll et al. would classify these all as Byzantine faults. A well-known occurrence in which an error message was misinterpreted as navigation data is the in-flight break-up of the first Ariane 5, Ariane Flight 501 [8]. Another example from another area of transportation is the grounding of the cruise ship Royal Majesty in 1995, in which incident the autopilot was designed in the expectation that the GPS would fail silent, but the GPS continued to send dead-reckoning data for over a day when it failed to receive a signal. The ship tracked 17 miles off course and grounded on Rose and Crown shoal near Nantucket Island, near Boston, MA [9,10]. The fault models of the system designers in the avionics case in [6], as well as in the Ariane 5 architecture and that of the STN Atlas NACOS 25 autopilot on the Royal Majesty, were inappropriate for the task.

There are various conclusions one can draw:

- * The kinds of numbers used in Fault Tree Analysis for random hardware failures in software-based systems give no good indication of the rate of systematic failures (due to design or to errors in software) which can be expected.
- * Fault-handling models are crucial parts of the architecture and their assumptions are critical. (This is made clear by the incidents

discussed
in [6,8,9].)

* That there have been no accidents does not mean that there are no occurrences of substantial problems with potentially catastrophic consequences with software-based critical avionics.

Acknowledgments

Thanks to John Sampson for pointing me to [2]; John Rushby for pointing me to [6]; Rod Chapman for pointing me to [8].

References

[1] World Airlines Directory, Flight International, 26 Oct - 1 Nov 2004.

[2] U.S. Federal Aviation Administration, AD 2005-18-51
Available at
http://www.airweb.faa.gov/Regulatory_and_Guidance_Library/rgad.nsf/0/25F9233FE09B613F8625706C005D0C53?OpenDocument

[3] Accidents and Incidents, Aviation Safety Week, 08 August 2005.

[4] Pease, M., Shostak, R., and Lamport, L., Reaching Agreement in the Presence of Faults, J. ACM 27(2): 228-234, 1980. Available from <http://research.microsoft.com/users/lamport/pubs/pubs.html>

[5] Lamport, L., Shostak, R., and Pease, M., The Byzantine Generals Problem, ACM Trans. Prog. Lang. Sys. 4(3): 382-401, 1982. Available from <http://research.microsoft.com/users/lamport/pubs/pubs.html>

[6] Driscoll, K., Hall, B., Sivencrona, H., and Zumsteg, P., Byzantine Fault Tolerance, from Theory to Reality, in S. Anderson, M. Felici and B. Littlewood, eds, Computer Safety, Reliability, and Security, 22nd

International Conference, SAFECOMP 2003, Edinburgh, UK, September 23-26, 2003, Book series Lecture Notes in Computer Science No. 2788, Springer-Verlag, 2003. Available from http://www.ce.chalmers.se/old/staff/sivis/articles/Safecomp_2003_revised.pdf

[7] Lloyd, E., and Tye, W., Systematic Safety, U.K. Civil Aviation Authority Publications, 1982.

[8] O'Halloran, C., Ariane 5: Learning from Failure, in J. Bowen and J. Woodcock, eds, Proceedings of the Grand Challenge 6 Workshop on Dependable Systems Evolution, at Formal Methods '05 conference, 18 July 2005, Newcastle-upon-Tyne. Available at <http://www.fmnet.info/gc6/fm05/proceedings.pdf>

[9] Heidiecker, L., Hoffmann, N., Husemann, P., Ladkin, P. B., Paller, J., Sanders, J., Stuphorn, J., Vangerow, A., WBA of the Royal Majesty Accident, RVS-RR-03-01, RVS Group, University of Bielefeld, 1 July 2003. Available from www.rvs.uni-bielefeld.de -> Publications -> Research Reports.

[10] U.S. National Transportation Safety Board, Marine Accident Report, Grounding of the Panamanian Passenger Ship Royal Majesty on Rose and Crown Shoal near Nantucket, Massachusetts, June 10, 1995. Report Number NTSB/Mar-97/01. Available from <http://www.nts.gov>

Peter B. Ladkin, University of Bielefeld, Germany www.rvs.uni-bielefeld.de

✦ Ships relying on GPS-based systems

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>

Wed, 31 Aug 2005 13:57:18 +0200

(was: US Navy to drop paper charts, Lichtensteiger, [RISKS-24.02](#))

> For commercial shipping, with it's much smaller crews, and
civilian

> sailors, the level of faith placed in a GPS and chartplotter
scares me.

The cruise ship Royal Majesty ran aground off Nantucket Island in 1995. The crew had been relying for over a day on an autopilot taking readings from a GPS position sensor. The GPS signal had been lost, supposedly thanks to the aerial being inadvertently disconnected, shortly after setting off from Bermuda, and the sensor was giving information through dead reckoning. It seems no one noticed, despite having a Loran available as a cross check. Also, the auto pilot error-handling was based on the GPS sensor being fail-silent, which was an incorrect assumption.

During the last hours, tracking some 17 miles off course, into known dangerous shallow waters, various obvious signals were ignored (white and "confused" water ahead; static shore lights sitting in the middle of the "ocean") as well as misidentification, and failure of identification, of buoys. The ship ran aground on Rose and Crown shoal and needed to be salvaged.

The report is on the U.S. NTSB WWW site. Slides from a talk, as well as a paper, giving a Why-Because Analysis of the accident may be

found at

www.rvs.uni-bielefeld.de -> Bieleschweig Workshops -> Second
Workshop ->
Talks

Thanks to Luke Emmet of Adelard for suggesting this as a case
study in 2002.

Peter B. Ladkin, University of Bielefeld, Germany www.rvs.uni-
bielefeld.de

VT Gas pumps give up at \$3/gallon

<Monty Solomon <monty@roscom.com>>

Sat, 3 Sep 2005 14:09:31 -0400

1% of Vermont's 6,000 gas pumps are unable to compute with gas
prices over
\$2.99. [PGN-ed from an Associated Press item, 3 Sep 2005]
[http://www.boston.com/news/local/articles/2005/09/03/
for_some_pumps_3_doesnt_compute/](http://www.boston.com/news/local/articles/2005/09/03/
for_some_pumps_3_doesnt_compute/)

UK Elections: Web and text vote trials dropped

<Chris Leeson <chris.leeson@atosorigin.com>>

Wed, 7 Sep 2005 10:10:34 +0100

Government plans to introduce e-voting for next year's local
council
elections have been dropped. According to the government
spokesman
(Elections Minister Harriet Harman), "the time is not right".
The
government has not ruled out further attempts to introduce e-

voting. Oliver Heald MP, Shadow Secretary of State for Constitutional Affairs, has described the whole process as a shambles, citing the security concerns with e-voting.

BBC News: http://news.bbc.co.uk/1/hi/uk_politics/4219008.stm

The Register: http://www.theregister.com/2005/09/06/govt_voting/

German social services software with new, costly errors

<Debora Weber-Wulff <D.Weber-Wulff@fhtw-berlin.de>>

Tue, 06 Sep 2005 09:06:53 +0200

In the never-ending tale of woe surrounding the German social services and unemployment software A2LL (produced by T-Systems, the software arm of the former German state Telecom company), the Spiegel has just reported that the software miscalculates the health insurance premiums that the government pays every month - to the tune of 25 million Euros too much, every month. The bill is footed by the taxpayers, of course, since T-Systems wisely put a cap in to contract for reparations - a maximum of 5 million Euros is all T-Systems needs to pay:

Spiegel: <http://www.spiegel.de/wirtschaft/0,1518,372998,00.html>

Tagesschau:

http://www.tagesschau.de/aktuell/meldungen/0,1185,OID4712732_REF2,00.html

Tagesspiegel:

<http://archiv.tagesspiegel.de/archiv/06.09.2005/2035255.asp>

Wikipedia for more background information on A2LL:

<http://de.wikipedia.org/wiki/A2LL>

According to *Der Spiegel*, an expert commission is already discussing what to do with the software, which was taken into service just in January of 2005. It has been declared to be in such a state of non-maintainability and non-adaptability ("nicht mehr wartungs- und entwicklungsfähig") that they are speaking about an entirely new software - to be written, of course, by T-Systems, who brought on this mess in the first place. They just are trying to decide whether to start a new central "solution" or a decentralized one for each unemployment office, as there are many local rules and insurance providers that seem to be causing difficulty.

The problem is with the insurance premiums for the unemployed, which was lowered retrospectively to save money for the government in March. A health insurance umbrella organization, VdAK, says it has difficulty in determining how much to pay back, if anything, because they do not know for exactly which people and months the wrong premium was calculated. A previous large error reported completely wrong data on who exactly was insured when to the insurance companies. The VdAK has said that when the German Social Services BA (Bundesagentur für Arbeit) gets their software straightened out, they will be glad - for a fee, of course - to see if they can repay the premiums paid in error. (In other news, the health insurance companies reported a surprise surplus recently...)

Even with the error now known, the software will not be able to

be fixed
this year at all [the last time I looked we had about a third of
a year
left....-dww], although it seems that just the rate for the
premiums needs
to be adjusted from 14.3% to 13.2%. The problem seems to stem
from there
being hundreds of different insurance providers, all with
slightly different
premium calculations.

See [RISKS-23.53](#), 23.60, 23.92.

Prof. Dr. Debora Weber-Wulff FHTW Berlin, FB 4, Internationale
Medieninformatik
Treskowallee 8, 10313 Berlin +49-30-5019-2320 weberwu@fhtw-
berlin.de

⚡ Not guilty because of system deficiencies

<Debora Weber-Wulff <D.Weber-Wulff@fhtw-berlin.de>>

Wed, 31 Aug 2005 18:14:00 +0200

The Berlin newspaper Tagespiegel reports on a curious court case:
<http://archiv.tagesspiegel.de/archiv/31.08.2005/2022942.asp#art>

Seems that a social worker found a neat way to dole out funds to
himself a
few years ago. [And yes, Peter, the pun is intentional! --dww]

Social services have a money machine set up in which, when a
client is given
money, instead of having it transferred to their account, a chip
card is
selected, and the number of the card typed into a computer
program that
controls payouts. The client takes the card to an ATM-like money
machine,

puts the card in, key is the secret password which is [I hope you are sitting down... --dww] the *birthday* of the client, and takes out the money. A camera films the transaction, but erases the tapes about 6 weeks later.

The program records the payout in the files of the client, and only people with proper passwords have access to the payout system. This is called security.

About 27.000 Euros (about the same in dollars these days) disappeared about 2 years ago. The revision department nailed down 22 transactions that had been conducted without an entry in the files of a client, and the clients knew nothing of the windfalls.

The accused kept his mouth shut during the process, and it was uncovered that the cards were not kept track of and "flew around the offices", people would log onto their payout computers and remain logged in all day, sometimes leaving the office without locking the door. It would have been trivial for a colleague to quickly use a computer to load up a card, then slip it to an accomplice and have them pick up the cash. In addition, everyone seemed to know everyone else's passwords...

The defence lawyer also noted that the social workers were all mad about the extra work they had to do about the new German dole system, so it really could have been anyone.

Berlin remains out the 27.000 Euros and has to pay court costs,

the accused
keeps his job (but was transferred, probably to the filing
room), and the
judge recommends they re-think the security of the payout
system. I'm with
the judge on this one!

Prof. Dr. Debora Weber-Wulff
FHTW Berlin, FB 4, Internationale Medieninformatik
Treskowallee 8, 10313 Berlin
Tel: +49-30-5019-2320 Fax: +49-30-5019-2300
weberwu@fhtw-berlin.de [http://www.f4.fhtw-berlin.de/people/
weberwu/](http://www.f4.fhtw-berlin.de/people/weberwu/)

⚡ The FBI Virtual Case File and other disasters

<jhhaynes@earthlink.net>

Mon, 5 Sep 2005 20:24:08 -0500 (CDT)

The September issue of *IEEE Spectrum* has a number of articles
of interest

to comp.risks readers. Cover story about why the VCF project
failed.

Article about Praxis High-Integrity Systems in Bath, England,
where they use

formal methods to ensure program correctness. And an article on
why

software fails, including a list of 31 projects from 1992 to
2005 that

failed after billions had been spent.

⚡ Mercedes car-door locking functionality

<"Leon Kuunders" <leon@kuunders.info>>

Sat, 13 Aug 2005 00:56:48 +0200

Last week I watched the chauffeur of a Mercedes car. There was a parking spot left just in front of another Mercedes. Both different types, though fairly new. As I watched by the chauffeur got out of her car and pushed the button on the remote control to close the doors.

The system worked. The doors of the Mercedes closed. The already parked Mercedes responded with a happy 'click' and opened it's doors. The chauffeur, confident the click was her car telling everything was fine, didn't pay attention, until I pointed her to the fact that she opened the other Mercedes.

She tried several times. When her car opened the other one closed. And vice versa. But she didn't see it as a problem, she could close the doors of her car and walk away. Until I pointed out the system probably worked the other way round as well ...

✉ **Re: Risks of Bluetooth pirates? (Kramer, [RISKS-24.02](#))**

<vp@cs.drexel.edu (Vassilis Prevelakis)>
Mon, 29 Aug 2005 22:14:58 -0400 (EDT)

> [...] the claimed modus operanti seems unlikely as short range
> wireless would be inactive unless the laptops were powered on
[...]

Actually my Apple G4 laptop has an entry in the Bluetooth

properties to allow Bluetooth devices to wake up the computer. This is to enable the user to move a Bluetooth mouse or press a key on a Bluetooth keyboard to wake up the laptop.

Of course, Bluetooth-enabled PDAs and cellphones are also at risks since these also respond to Bluetooth queries unless the feature has been turned off by the user.

First generation Bluetooth devices imposed a significant burden on the battery of a portable device which is why the user was made more aware of the wireless network (prominent annunciators indicating Bluetooth activity etc.). Newer Bluetooth devices can operate in very low power mode (light sleep) so they can be left turned on continuously. As the power requirements are decreased further, Bluetooth activity may become "transparent" to the user resulting in another silent feature can bite unsuspecting users.

Vassilis Prevelakis, Ph.D., Computer Science Department, Drexel University,
Philadelphia, PA 19104-2875 <http://vp.cs.drexel.edu> +1 215-895-2920



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 4

Friday 16 September 2005

Contents

- [Nation's Critical Infrastructure Vulnerable to Cyber Attack](#)
[U.S. House Science Committee](#)
- [Katrina -- predictions before and response after](#)
[Inman Harvey](#)
- [Health Records Of Evacuees Go Online](#)
[Jonathan Krim](#)
- [One radio frequency for emergency services](#)
[Fred Cohen](#)
- [LA power outage](#)
[PGN](#)
- [Public Call for Skype to Release Specifications](#)
[Lauren Weinstein](#)
- [WebGoat 3.7 - Application Security hands-on learning environment](#)
[Jeff Williams](#)
- [National Academies/CSTB report on Electronic Voting](#)
[Herb Lin](#)
- [Gmail security flaw: acts on javascript in unopened e-mail](#)
[Suw Charman](#)

- [Re: Risks of REAL ID: incorrect](#)
[Steven M. Bellovin](#)
 - [CardSystems Complies With Industry Standards](#)
[Curt Sampson](#)
 - [REVIEW: "Forensic Discovery", Dan Farmer/Wietse Venema](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Nation's Critical Infrastructure Vulnerable to Cyber Attack

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

Fri, 16 Sep 2005 07:59:39 PDT

Committee on Science, SHERWOOD BOEHLERT, CHAIRMAN

Bart Gordon, Tennessee, Ranking Democrat

<http://www.house.gov/science/press/109/109-129.htm>

Press Contacts: Joe Pouliot (202) 225-4275

WASHINGTON, D.C., September 15, 2005 - In testimony before the House Science Committee today, the Chief Information Officers (CIOs) of major U.S. corporations warned Congress that the nation's critical infrastructure remains vulnerable to cyber attack. The witnesses said the economy is increasingly dependent on the Internet and that a major attack could result in significant economic disruption and loss of life.

Urging action to address this vulnerability, the witnesses advocated increased funding for cybersecurity research and development (R&D) and greater information sharing between industry and government and among various sectors of industry. Witnesses also urged greater federal attention

to cybersecurity and praised the creation of an Assistant Secretary for Cybersecurity at the Department of Homeland Security (DHS).

Testifying before the Committee were: Mr. Donald "Andy" Purdy, Acting Director, National Cyber Security Division, Department of Homeland Security; Mr. John Leggate, Chief Information Officer, British Petroleum Inc.; Mr. David Kepler, Corporate Vice President, Shared Services, and Chief Information Officer, The Dow Chemical Company; Mr. Andrew Geisse, Chief Information Officer, SBC Services Inc.; and Mr. Gerald Freese, Director, Enterprise Information Security, American Electric Power.

"We shouldn't have to wait for the cyber equivalent of a Hurricane Katrina to realize that we are inadequately prepared to prevent, detect and respond to cyber attacks," said Science Committee Chairman Sherwood Boehlert (R-NY).

"And a cyber attack can affect a far larger area at a single stroke than can any hurricane. Not only that, given the increasing reliance of critical infrastructures on the Internet, a cyber attack could result in deaths as well as in massive disruption to the economy and daily life.

"So our goal this morning is to help develop a cybersecurity agenda for the federal government, especially for the new Assistant Secretary. I never want to have to sit on a special committee set up to investigate why we were unprepared for a cyber attack. We know we are vulnerable, it's time to act."

Legate testified that an informal survey earlier this year found that

executives in the telecommunications, energy, chemical, and transportation sectors estimated that about 30 percent of their revenue depends directly on the Internet. He also said that, because of interdependency among various industry sectors, a single attack could reverberate throughout the global economy: "These cascading dependencies all too quickly create 'domino effects' that are not obvious to the corporate customer or the policymaker."

Kepler told the Committee that the greatest concern for the chemical industry is the potential for a combined cyber and physical attack. He said he fears a potential terrorist "using information on shipments, product inventory, or sites to construct a physical attack.using false identity to acquire chemicals for improper use, [or].gaining inappropriate access to systems to cause isolated disruptions."

To help prevent these scenarios from being realized, Kepler urged greater industry input in the government's critical infrastructure protection efforts. "Information sharing and continued cooperation between our sector and the Department of Homeland Security is critical," he testified. "Above all else, efforts must be focused on those threats of greatest impact and concern to our national security, while addressing the unique needs of each sector."

Freese said the security of his sector could also be enhanced through increased coordination with federal agencies, such as DHS. He also urged

greater R&D funding to guide the development of a next generation Internet and a generation power grid system that will have built-in security features to protect against cyber attacks. "The long term solution to present inadequacies is to build out the old infrastructure with the next generation of technologies and equipment. The new infrastructure will be based on greater levels of security and reliability, enhanced design, and recognition of the interdependencies between the electricity sector and the communications sector."

The industry witnesses praised the creation of the Assistant Secretary position and said it will result in greater attention to cybersecurity issues. Geisse also urged DHS to continue its focus on cyber-related activities that have proven successful. He said, "We encourage the Department of Homeland Security to continue to: support research grants and assistance that focus on national cybersecurity; support industry organizations and government agencies that create security standards and best practices; provide early warnings of security events through various government agencies; and make sure the security best practices that various critical government agencies develop are shared with our critical infrastructure industries."

109-129

Katrina -- predictions before and response after

<Inman Harvey <inmanh@cogs.susx.ac.uk>>

Thu, 08 Sep 2005 10:51:44 +0100

They told you so (2002):

- SPECIAL REPORT from THE TIMES-PICAYUNE -

It's only a matter of time before South Louisiana takes a direct hit

from a major hurricane. Billions have been spent to protect us, but we

grow more vulnerable every day.

Five-Part Series published June 23-27, 2002

<http://www.nola.com/hurricane/?/washingaway/>

They told you so (2004)

What if Hurricane Ivan Had Not Missed New Orleans? Disasters Waiting to

Happen . . . Sixth in a Series Natural Hazards Observer, 2 November 2004

<http://www.colorado.edu/hazards/o/nov04/nov04c.html>

A couple of examples from many on

<http://en.wikipedia.org/wiki/>

[Predictions of hurricane risk for New Orleans](#)

What use are calculations and predictions of risk, without the institutions

and the political will to react to them? From a viewpoint outside the US,

the response to the Katrina disaster has been quite frankly unbelievable --

sending in troops with guns as a priority over medical and humanitarian

assistance being the most bizarre.

The really big risk is the deep-seated systemic and institutional malaise for which such responses are symptoms. This is far more than

merely a hurricane.

Inman Harvey, Evolutionary and Adaptive Systems Group, COGS/
Informatics,

Univ. of Sussex, Brighton BN1 9QH, UK <http://www.cogs.susx.ac.uk/>

[users/inmanh/](#)

🔥 Health Records Of Evacuees Go Online (Jonathan Krim)

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

Wed, 14 Sep 2005 19:46:58 PDT

The federal government is making medical information on Hurricane Katrina evacuees available online to doctors, the first time private records from various pharmacies and other health care providers have been compiled into centralized databases. The data contain records from 150 Zip codes in areas hit by Katrina. Starting yesterday, doctors in eight shelters for evacuees could go to the Internet to search prescription drug records on more than 800,000 people from the storm-racked region. Officials hope to soon add computerized records from Medicaid in Mississippi and Louisiana, Department of Veterans Affairs health facilities, laboratories and benefits managers.

The records are one step in reconstructing medical files on more than 1 million people disconnected from their regular doctors and drug stores. Officials fear that many medical records in the region, especially those that were not computerized, were lost to the storm and its aftermath.

Although the immediate focus is on urgent care for hurricane victims, participants in the effort say the disaster demonstrates a broader need to

computerize individual health records nationwide and make them available throughout the medical system. Such a step could, for example, give emergency room doctors a way to quickly view medical histories for late-night accident victims.

Electronic health records are controversial among many privacy advocates, who fear the data could be exploited by hackers, companies or the government. [Source: Jonathan Krim, Government Wants Doctors in Shelters to Have Data, *The Washington Post*, 14 Sep 2005, A24; Thanks to Keith A Rhodes. PGN-ed. The article has considerable discussion on the privacy implications.]

✶ One radio frequency for emergency services

<Fred Cohen <dr.cohen@mac.com>>

Sun, 11 Sep 2005 18:59:01 -0700

It is sad that politicians start to believe that they know how to solve technical problems. One such sad case was Rudy Giuliani's pronouncement today that a single frequency (then frequency band) for all emergency services would make things work better. Now I am hardly the world's leading expert on radio frequency spectrum allocation, but I do have some small amount of experience in understanding radio communications and emergency response, and I was startled, well not all that startled, perhaps bemused at the lack of understanding displayed by people who are not risk

management

professionals. Of course it seems that a lot of political folks think that they can do as good a job as risk management professionals, and likely that is why we are in such a sad state as a nation state at handling emergencies.

I haven't done a complete assessment of the suggestion, but here are some initial thoughts.

The idea is that communications will work better if everyone can talk to each other and therefore a single frequency band would allow them to do so and improve emergency communications. Sounds sensible, however...

1) It means that in order to disrupt ALL emergency communications I only need to jam one frequency band.

2) Different natural and artificial phenomena interfere with RF communications in different frequency bands, so by using a relatively limited portion of the available bandwidth, there is a guarantee that in some places no communications will work.

3) If I want to listen into your communications, it makes it a lot easier if I know the frequencies being used, and if everyone has to talk to each other, then anyone can listen to everyone else. Encryption won't solve this of course for the same reason.

4) If there is a big emergency and everyone is on a small subset of the bands available, there will be a lot of interference, reducing communications effectiveness.

5) Certain weather and other human induced conditions wipe out portions of

the frequency band for periods of time, making ALL communications fail simultaneously (see 1 above).

6) Interference between jurisdictions means that dispatchers in one jurisdiction might end up talking over those of their neighbors, causing confusion and more traffic problems as well as increasing the potential for phony messages going on the air.

You all get the idea by now. Of course the last assessment I did that involved a radio communications system for a local government was several weeks back, and we were a bit concerned that they only had 3 redundant ways to communicate via RF - Car radios that talk to towers in redundant locations - hand-held radios on a different frequency range that could talk to the towers, the cars, and each other independently of the other tower system, and cellular telephones that they could use when the other systems failed. They also reported problems of interference on rare occasions with the frequencies used by neighboring jurisdictions (see 6 above), but only in certain locations where they could communicate over quite a long distance because of weather-related signal bounces off of clouds.

Different frequency bands are used for different things for good reasons, and there are good reasons that a single frequency band for emergency response would be a bad thing. Perhaps we should put Rudy in charge of FEMA and see if things get better or worse... after all, the last political appointee there with no expertise in emergency management worked

out so
well...

Security Posture <http://securityposture.com>; University of New
Haven;
Fred Cohen & Associates 1-925-454-0171 Security Management
Partners

[Further discussion at iwar@yahoogroups.com, including whether
one
frequency or one frequency band was intended. PGN]

LA power outage

<"Peter G. Neumann" <neumann@csl.sri.com>>
Mon, 12 Sep 2005 16:28:43 PDT

About 700,000 electric customers in Los Angeles lost power
Monday afternoon
(12 Sep 2005) after a worker mistakenly cut a wrong line,
triggering a
cascade of problems in the city's power grid, a spokesman for
the Los
Angeles Department of Water and Power said. [The latest report
as this
issue goes out is that the spec for the operation was incorrect,
and that
the crew did exactly as they had been told. PGN]

Public Call for Skype to Release Specifications

<Lauren Weinstein <lauren@vortex.com>>
Mon, 12 Sep 2005 14:47:24 -0700

As I noted in:

<http://lists.elistx.com/archives/interesting-people/200509/msg00122.html>

eBay's acquisition of Skype (now official) leads to new concerns over the proprietary nature of Skype's security and encryption systems, which will now be under the control of an extremely large and powerful corporate entity.

For eBay and Skype to have a chance of maintaining the goodwill and trust of Skype users, I call on Skype to forthwith release the specifications and implementation details of Skype's encryption and related technologies.

This disclosure should ideally be made to the public, but at a minimum to an independent panel of respected security, privacy, and encryption experts, who can rigorously vet the Skype technology and make a public report regarding its security, reliability, and associated issues.

There are also other significant concerns regarding this acquisition, relating to eBay's privacy policies and how they may impact the privacy of Skype users, but I'll hold those for a future message.

Lauren Weinstein lauren@pfir.org 1 818-225-2800
<http://www.pfir.org/lauren> <http://www.eepi.org> <http://daythink.vortex.com>

environment

<"Jeff Williams" <jeff.williams@owasp.org>>

Tue, 6 Sep 2005 09:56:11 -0400

[From SC-L, included in RISKS with permission of the author.
PGN]

The **only** way to learn application security is to test applications "hands on" and examine their source code. To encourage the next generation of application security experts, the Open Web Application Security Project (OWASP) has developed an extensive lesson-based training environment called "WebGoat".

WebGoat is a lessons based, deliberately insecure web application designed to teach web application security. Each of the 25 lessons provides the user an opportunity to demonstrate their understanding by exploiting a real vulnerability. WebGoat provides the ability to examine the underlying code to gain a better understanding of the vulnerability as well as provide runtime hints to assist in solving each lesson. V3.7 includes lessons covering most of the OWASP Top Ten vulnerabilities and contains several new lessons on web services, SQL Injection, and authentication.

WebGoat 3.7 is available for free download from:

<http://www.owasp.org/software/webgoat.html>

Simply unzip, run, and go to WebGoat in your browser to start learning.

The OWASP Foundation is dedicated to finding and fighting the

causes of
insecure software. Find out more at <http://www.owasp.org>.

⚡ National Academies/CSTB report on Electronic Voting

<"Herb Lin" <HLin@nas.edu>>

September 13, 2005 10:31:17 PM EDT

Announcing a new report from CSTB on Electronic Voting. Below is the media advisory on it. [Reproduced from Dave Farber's IP list.]

Election officials across the United States are increasingly looking to electronic voting systems as a way to administer elections more efficiently, but skeptics have raised concerns about the security and reliability of these systems. ASKING THE RIGHT QUESTIONS ABOUT ELECTRONIC VOTING, new from the National Academies' National Research Council, offers a set of questions that policy-makers and the public should ask to help ensure that the technologies implemented are secure, reliable, efficient, and easy to use. Advance copies are now available to reporters. The report, which was chaired by DICK THORNBURGH, former governor of Pennsylvania, and RICHARD F. CELESTE, former governor of Ohio, was released on September 13, 2005, and is available free in PDF form at the web site below.

Press release at <http://www4.nationalacademies.org/news.nsf/isbn/0309100240?OpenDocument>

Full report at <http://www.nap.edu/catalog/11449.html> (sign-in

required for the PDF version).

Herb Lin, Senior Scientist and Study Director, CSTB
National Academies, 1-202-334-3191

🔥 Gmail security flaw: acts on javascript in unopened e-mail

<Suw Charman <suw.charman@gmail.com>>

Fri, 16 Sep 2005 09:36:37 +0100

I received a spam this morning that opened audio files without me even opening the e-mail. The spam was from 'news@capitalex.com' and had the subject 'news'.

A closer look reveals this code:

```
<Script Language='Javascript'>
```

```
<!--
```

```
document.write(unescape('%3C%49%46%52%41%4D%45%20%77%69%64%74%68%3D%22%31%22%20%68%65%69%67%68%74%3D%22%31%22%20%53%52%43%3D%22%68%74%74%70%3A%2F%2F%77%77%77%2E%70%72%6F%66%6F%72%65%78%74%72%61%64%65%2E%63%6F%6D%2F%69%6D%61%67%65%73%2F%6E%65%77%65%78%2E%68%74%6D%6C%22%20%66%72%61%6D%65%42%6F%72%64%65%72%3D%22%31%22%20%0D%0A%0D%0A%73%63%72%6F%6C%6C%69%6E%67%3D%22%6E%6F%22%3E%3C%2F%49%46%52%41%4D%45%3E' ));
```

```
//-->
```

```
</Script>
```

This decodes to

```
<IFRAME width="1" height="1"  
SRC="http://www.proforextrade.com/images/newex.html"
```

```
frameBorder="1"  
scrolling="no"></IFRAME>
```

That page loads automatically, *without me having opened the e-mail*, then runs a shed load of rubbish including two audio files.

Full e-mail with headers available on request.

⚡ **Re: Risks of REAL ID: incorrect (Re: [RISKS-24.02](#))**

<Steven M. Bellovin" <smb@cs.columbia.edu>>
Mon, 29 Aug 2005 12:03:15 -0400

Charles Lamb's comment on the REAL ID law, though technically correct, is disingenuous. A National Research Council report ("Who Goes There -- Authentication Through the Lens of Privacy") noted this:

Finding 6.5: State-issued driver's licenses are a de facto nationwide identity system. They are widely accepted for transactions that require a form of government-issued photo ID.

Steven M. Bellovin, <http://www.cs.columbia.edu/~smb>

⚡ **CardSystems Complies With Industry Standards**

<Curt Sampson <cjs@cynic.net>>
Fri, 2 Sep 2005 13:43:11 +0900 (JST)

At either of these two URLs:

<http://xrl.us/hd9g>

[http://yahoo.reuters.com/financeQuoteCompanyNewsArticle.jhtml?
duid=mtfh39850_2005-09-01_15-31-19_n01450451_newsml](http://yahoo.reuters.com/financeQuoteCompanyNewsArticle.jhtml?duid=mtfh39850_2005-09-01_15-31-19_n01450451_newsml)

you can read that

Payments processor CardSystems Solutions Inc., where a security breach

exposed more than 40 million credit card accounts to fraud, on Thursday

said its auditor had completed a report to payment networks and concluded

it complies with industry data-security standards.

The sad thing is, it's probably true.

Curt Sampson <cjs@cynic.net> +81 90 7737 2974 [http://www.
NetBSD.org](http://www.NetBSD.org)

⚡ REVIEW: "Forensic Discovery", Dan Farmer/Wietse Venema

<Rob Slade <rslade@sprint.ca>>
Wed, 14 Sep 2005 08:16:39 -0800

BKFORDIS.RVW 20050310

"Forensic Discovery", Dan Farmer/Wietse Venema, 2005, 0-201-63497-X,

U\$39.99/C\$57.99

%A Dan Farmer zen@fish2.com

%A Wietse Venema wietse@porcupine.org

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8

%D 2005

%G 0-201-63497-X

%I Addison-Wesley Publishing Co.

%O U\$39.99/C\$57.99 800-822-6339 Fax: (617) 944-7273

bkexpress@aw.com

%O [http://www.amazon.com/exec/obidos/ASIN/020163497X/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/020163497X/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/020163497X/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/020163497X/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/020163497X/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/020163497X/robsladesin03-20)

%O Audience a+ Tech 3 Writing 1 (see revfaq.htm for explanation)

%P 217 p.

%T "Forensic Discovery"

In the preface, the authors don't promise to teach the reader anything about computer or digital forensics. Rather, they are reporting on ten years' worth of experience in looking into attacked machines. Given the authors' background, this is engrossing. But turning it into useful guidance might be left as an exercise for the reader. This is not a tutorial work for the novice, but a challenge to the experienced professional.

Part one outlines the basic concepts of forensics in digital systems.

Chapter one presents the "spirit of forensic discovery": look anywhere, for anything, and be prepared when you find it. (This is a tall order, particularly the "being prepared" part, but it basically corresponds to my experience.) Time information and stamps (on UNIX systems) are discussed in chapter two, along with mention of the ways that clumsy attempts to "save" systems can destroy ephemeral information. However, the level of the material sweeps between broadly generic and tightly specific: it may be difficult for those not already thoroughly familiar with forensic activities

to obtain useful guidance from it.

Part two is supposed to provide us with background on the abstractions of the computer and operating systems that relate to forensic recovery of materials. Chapter three addresses file system basics, but does so specifically with regard to the UNIX system. The content is much more detailed than conceptual (covering, for example, allowable characters in UNIX filenames), and command examples are not always completely explained. The usefulness of this approach is questionable, since the reader is assumed to know the UNIX system well; in which case, why cover the elementary fundamentals? However, the work does highlight aspects of operating and file system internals not encountered in normal administrative activity. Analysis of information recovered from a compromised system is reviewed in chapter four. The methods and procedures are very strictly limited by the case cited, but the examples demonstrate the backhanded thinking needed to obtain interesting data after an intrusion. A variety of intriguing ways to subvert a running system are examined in chapter five. As with previous material, the text seems to talk around the topic, while the examples, although fascinating, don't always support the general concepts under discussion. Analysis of the code of malicious software (a practice known in virus research as forensic programming) is addressed in chapter six, although the bulk of the content deals with test execution of the programming (under various forms of restriction) and both the benefit and

complexity of disassembly is passed over rather lightly.

Part three moves beyond the concepts and into practical difficulties.

Chapter seven, although titularly about the contents of deleted files, is

primarily concerned with the conservation and preservation of the access,

modification, and (attribute) change times of files. (In response to the

draft of this review, the authors clarified some of the points that they

were trying to make in the text, such as the fact that material from deleted

files is often more persistent than the content of active files.

Unfortunately, these points, while arresting, are not always clear in the

work itself.) Retrieving data from memory, particularly via the swap or

paging areas of disk, is reviewed in chapter eight.

The preface does state that the authors intend this book to be useful to

sysadmins, incident responders, computer security professionals, and

forensic analysts. I would suggest that only the last group will find much

here that they can use, and then only those at the advanced edges of the

field. There is certainly much that is intriguing, but the material demands

of the reader that he or she have extensive background and knowledge of

system and filesystem internals. Even then, extracting the information from

the target system, and drawing conclusions as to the implications of that

data, will be difficult. Farmer and Venema have outlined some fascinating

material, on the bleeding edge of the technology, but have not made it easy

for practitioners to utilize or comprehend.

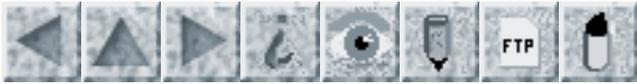
(In response to the draft review, The authors have noted that the full, original text of the book is now available at <http://fish2.com/forensics/> or [http://www.porcupine.org/forensics/.](http://www.porcupine.org/forensics/))

copyright Robert M. Slade, 2005 BKFORDIS.RVW 20050310
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.
niu.edu
<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>

[I found this book to be very useful, timely, and interesting. 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

Search RISKS using [swish-e](#)

Volume 24: Issue 5

Friday 30 September 2005

Contents

- [Software hijacks jet airliner ... again?](#)
[Charles Wright](#)
- [Airbus, Whistleblower Dispute A380 Pressurization Controls](#)
[PGN](#)
- [Metra Rail accident in Chicago](#)
[Andy Steingruebl](#)
- [Katrina victims required to use Microsoft IE](#)
[Douglas W. Jones](#)
- [Travelers Continue to Struggle with Wrongful Watch List Matches](#)
[EPIC FOIA Notes](#)
- [Scots Jail hi-tech door locking system broke](#)
[George Michaelson](#)
- [Risks of keyboard shortcuts](#)
[Andrew Koenig](#)
- [Designing "safe software" ...: A 4-star article!](#)
[Michael Radow](#)
- [Sorcerer's Apprentice in the Driver's Seat??](#)
[David Lesher](#)

- [Mea culpa: How we got it wrong on Calling-Number ID](#)
[Geoff Kuenning](#)
 - [Open letter: Why "dot-xxx" is for Chumps](#)
[Lauren Weinstein](#)
 - [Router worms and International Infrastructure](#)
[Gadi Evron](#)
 - [Wolf Blitzer repeats Rudy in questioning governors](#)
[Fred Cohen](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈ Software hijacks jet airliner ... again?

<"Charles Wright" <cw@pobox.com>>
Sat, 17 Sep 2005 11:26:11 +1000

http://www.bleedingedge.com.au/blog/archives/2005/09/software_hijack.html

The Australian (17 Sep 2005) has a chilling story about the pilots of a Malaysian Airlines 777 flying from Perth to Kuala Lumpur last month battling to regain control after an "unknown computer error" caused the aircraft to pitch violently, and brought it close to stalling.

An Australian Transport Safety Bureau report (http://www.atsb.gov.au/aviation/occurs/occurs_detail.cfm?ID=767) released

yesterday reveals the pilot in command disconnected the autopilot and lowered the plane's nose to prevent a stall, after incorrect data from a supposedly fail-safe device caused the plane to pitch up and climb 3000ft, cutting its indicated air speed from 500kmh to 292kmh, activating a stall

warning and a "stickshaker". [A stickshaker vibrates the aircraft's controls to warn the pilot when he is approaching stall speed ... which, you know, means the plane is about to fall out of the air.]

The system refused to give up control, however. It increased the power on the automatic throttle, forcing the pilot to counter by pushing the thrust levers to the idle position. The aircraft immediately pitched up again, and climbed 2000ft.

The pilot turned back to Perth under manual control. When he kicked in the two autopilot systems, the plane banked to the right, and the nose pitched down.

On its landing approach, at 3000ft, the flight display gave a low airspeed warning and the auto-throttle increased thrust. The warning system also indicated a dangerous windshear, but the crew landed the jet safely.

According to the report, "investigations are focusing on faulty acceleration figures supplied by a device called the Air Data Inertial Reference Unit". The ADIRU collates aircraft navigation and performance data from other systems and passes the information to the primary flight computer.

What's potentially more disturbing, however - and neither the Transport Safety Bureau nor The Australian appear to have picked this up - is that a US FAA directive (http://www.airweb.faa.gov/Regulatory_and_Guidance_Library%5CrgAD.nsf/0/A668AA4EB82ABE4E86256FFE00510CE8?OpenDocument)

in June this year highlighted other problems with the Boeing 777's ADIRU.

Boeing has told operators of the jet -- which by the way has the best safety record of any aircraft (http://www.geocities.com/khlim777_my/ashowsafe1.htm)

-- to load a previous software version.

[The article at

<http://www.avweb.com/eletter/archives/avflash/465-full.html>

was also noted by Mickey Coggins and Ian Chard.

<http://www.theaustralian.news.com.au>

was cited by Richard Weir. PGN]

✦ Airbus, Whistleblower Dispute A380 Pressurization Controls

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

Tue, 27 Sep 2005 11:13:19 PDT

James Paul (U.S. House Science Committee professional staffer) called my attention to an item in the 27 Sep 2005 *Los Angeles Times*. A whistleblower alleges that the chips controlling cabin pressurization valves in Airbus's new Flying Whale aren't behaving properly and may lead to decompression incidents.

<http://www.latimes.com/news/printedition/front/la-fi-whistleblower27sep27,1,2186118.story>

✦ Metra Rail accident in Chicago

<Andy Steingruebl <steingra@gmail.com>>

Tue, 20 Sep 2005 09:40:22 -0500

As you are no doubt aware, there was a Metra Rail train accident in Chicago this last weekend that caused the death of two people and injured approximately 80. The issue has gotten national news coverage, and lots of local coverage. The Metra spokesperson has been rather forthcoming in analysing the situation.

Because the train was speeding at the time of the accident and the accident is similar to previous train accidents, there have been a lot of calls for solutions:

- Put a second person back in the train to help the engineer. There was a second person until 1995.
- Implement automated train controls to brake the train in case of an engineer missing a signal.

The second option has received a lot of attention because Metra currently has computer controls on several of its train lines, but the controls are expensive.

This situation presents a great opportunity to get the issue of the reliability of human and computer controls in the media. As the ideas are being widely discussed, its a perfect opportunity to discuss failure rates for the different technologies, the humans, etc.

I'd contact Metra Rail myself, but I don't have the requisite engineering

background to act as a truly knowledgeable source.

Perhaps you or someone from RISKS (perhaps someone in the Chicago area) can contact local news media and Metra to get this issue discussed in public as it should be.

[Added note: I believe it was going about 60 and the speed limit for that section of track was 10. Recent news is the the engineer either missed the signal, or the signal was green indicating he could keep his speed and not slow down. In either case since its a big news story. AS]

⚡ Katrina victims required to use Microsoft IE

<"Douglas W. Jones" <jones@CS.UIOWA.EDU>>

Thu, 22 Sep 2005 10:02:21 -0500

[In a USACM newsgroup, Barbara Simons noted that FEMA requires Katrina

evacuees to use Microsoft IE 6.0 for access to its website:

<http://www.groklaw.net/article.php?story=2005091305273070>

The following message by Doug Jones discusses that issue. PGN]

The FEMA web portal violates a number of good web usage guidelines. The first page at <http://fema.gov/> is fixed-width, not conforming to the user's browser window. Things get worse from there.

The web page <http://www.disasteraid.fema.gov/> is a mess when viewed under iCab, my preferred web browser, the browser spent what seemed an eternity blinking from grey to white and back again before stabilizing

with content.

When I clicked on Register for Assistance, it went back to blinking and kept it up for so long that I gave up.

When I repeated the exercise under Safari, Clicking on Register for

Assistance, which takes me to

<https://www.disasteraid.fema.gov/famsVuWeb/integration>

I got the following error message:

500 Internal Server Error

Servlet error: java.lang.ClassNotFoundException:

_dynamic._templates._Template__body

When I tried it under IE, it got farther, letting me through an automated test to distinguish humans from bots, but then it gave me

the message:

Integrated Security Access and Control (ISAAC) Unavailable

Your request cannot be processed because the ISAAC system is unavailable.

Please try again later or contact the FEMA Helpline at the number

listed below.

So, it's clear to me that they've engineered a web system that is:

a) Extraordinarily over-engineered to work under only one browser,

b) Nonfunctional under that browser,

This, I conclude, is simply another example of FEMA incompetence.

✶ Travelers Continue to Struggle with Wrongful Watch List Matches

<EPIC FOIA Notes <FOIA_Notes@epic.org>>

Tue, 27 Sep 2005 11:47:44 -0400

EPIC FOIA Notes #8:

Travelers Continue to Struggle with Wrongful Watch List Matches

Documents obtained by EPIC from the Transportation Security Administration

under the Freedom of Information Act reveal nearly a hundred complaints from

airline passengers between November 2003 and May 2004. The most common

complaint from passengers is that they have been wrongly placed on a

government watch list. Numerous complaints show passengers' frustration

with the agency's failure to resolve their misidentification problems.

More information: http://www.epic.org/foia_notes/note8.html

FOIA_Notes mailing list FOIA_Notes@mailman.epic.org

https://mailman.epic.org/cgi-bin/mailman/listinfo/foia_notes

✶ Scots Jail hi-tech door locking system broke

<George Michaelson <ggm@apnic.net>>

Tue, 20 Sep 2005 11:18:59 +1000

This one begs a few questions: How can the inmates have had over a *month*

of using the hackaround without other non-linked security systems (e.g., a

video cameras) not noticing?

This suggests that an integrated solution has replaced multiple discrete

lines of protection, with predictable outcomes. George

<http://news.scotsman.com/scotland.cfm?id=1965122005>

Prison officers have been forced to abandon a new security system and return to the use of keys after the cutting-edge technology repeatedly failed. The system, which is thought to have cost over £3 million, used fingerprint recognition to activate the locking system at the high-security Glenochil Prison near Tullibody, Clackmannanshire. ... For more than a month, the 420 inmates - including some murderers and other high-risk inmates - had been able to wander around the high-security jail. Staff claim that the unlimited access to all parts of the prison had allowed some prisoners to settle old scores with rivals.

George Michaelson, APNIC, PO Box 2131 Milton, QLD 4064 Australia
<http://www.apnic.net> ggm@apnic.net +61 7 3858 3150

⚡ Risks of keyboard shortcuts

<"Andrew Koenig" <ark@acm.org>>
Wed, 28 Sep 2005 10:44:32 -0400

Background: Microsoft Windows can support only 10 USB MIDI devices. This may sound like a lot until you realize that when you move a device to a different USB port, it counts as a new device. The list of devices is stored in the registry, using keys named "midi", "midi1", ... "midi9". I was running regedit to try to understand the degree to which these keys had become filled, and to delete some of the duplicates.

I turned away from the keyboard for a moment. When I turned back, on the screen was a dialog box saying "Do you want to permanently delete this key and all of its components? Yes/No", and one of my five-month-old kittens was ambling away from the keyboard.

I'm not usually a fan of such dialog boxes, but this time I'll make an exception--especially as regedit does not have an undo function. Yes, I know about system restore points, but still...

✶ Designing "safe software" ...: A 4-star article!

<Michael Radow <mikeradow@yahoo.com>>

Thu, 15 Sep 2005 19:36:33 -0700 (PDT)

David Kalinsky, Architecture of safety-critical systems
September issue of "Embedded Systems Programming" magazine
<http://www.embedded.com//showArticle.jhtml?articleID=169600396>
"compressed" URL <http://runurl.com/x.php?b0>

✶ Sorcerer's Apprentice in the Driver's Seat??

<"David Lesher" <wb8foz@panix.com>>

Sat, 17 Sep 2005 09:51:21 -0400 (EDT)

The driver of a runaway [21 ton] truck that locked at 60 mph for 140 miles on highways in northern France and Belgium is planning to sue the truck manufacturer. The crisis happened Monday when the driver, who

refused to

give his name, used his mobile phone to raise the alarm when he realized

he could not brake or change gears. ... {no good scheme to stop it;

finally skidded out} ... Iveco, the truck manufacturer, sent technicians

to examine the vehicle. The driver denies he was at fault and he was

taking legal action. [UPI item, abstracted]

A slew of Risks, here. First the obvious, did it go down as reported; i.e.,

the driver really had no way to stop it? (Or had he been to see <<http://us.imdb.com/title/tt0111257/>> recently.)

If so, why? Diesel vehicles usually have an emergency shutoff that blocks

the air intake. Was it NOT manually operable, or did it fail as well? And

were the brakes out, or insufficient to overcome the engine power?

It will be interesting to see the followup analysis.

✶ Mea culpa: How we got it wrong on Calling-Number ID

<Geoff Kuenning <geoff@cs.hmc.edu>>

25 Sep 2005 23:37:03 -0700

Back in the early 90's, U.S. phone companies began rolling out the service

known as "Caller ID" (really Calling Number ID, or CNID). Early adopters

were very pleased with the feature; it helped them to avoid telemarketers

and occasionally to dodge inconvenient friends.

Then a few privacy advocates noticed that there was a dark side:
if
you called a local business, it could capture your number with
CNID
and add you to a telemarketing list. Suddenly CNID changed from
a
beneficial service to a nefarious plot.

An anti-CNID campaign ensued, culminating in California's
decision to
require telephone companies to offer free CNID blocking as a
condition of
rolling out the service. At the same time, privacy advocates
(including me
and many other RISKS subscribers) publicized the downsides of
CNID:
unintentionally revealing your (possibly unlisted) phone number,
confusing
the concept of calling number with the identity of the calling
person, etc.
The campaign was successful: when CNID was rolled out, something
like 50% of
Californians chose to block their number by default.

Fast forward approximately a decade. I recently switched local
phone
providers (finally freeing myself from the clutches of Verizon,
né GTE,
after a 25-year quest) and got rid of my CNID blocking in the
process.
Rather than advocating against CNID, I've now changed my tune
and am trying
to convince my blocked friends to unblock.

What happened? The answer is simply that I was wrong about the
evils of
CNID, and wrong about the (perceived lack of) benefits. That
error arose
primarily from an inability to correctly predict the future. In
particular,
the following forces have reduced the evils and increased the
benefits:

1. The predicted data collection by small businesses never happened. It wasn't worth the effort. Businesses didn't get much benefit from knowing that somebody at 555-1234 had called to inquire about mattress prices; their telemarketing money was better spent on buying phone lists that included names and demographic data.
2. Larger businesses had 800 numbers that included Automatic Number Identification (ANI), which wasn't bothered by caller ID blocking anyway, so the people with lots of funds were never stopped from telemarketing.
3. The unforeseen Federal Do-Not-Call List has become an effective defense against telemarketing, so revealing your telephone number isn't much of a problem anyway.
4. The rise of cellphones means that we are starting to see a true one-to-one association between phone numbers and people, so CNID is becoming the caller ID it was once billed as being.
5. Most cellphone plans include CNID as part of the package, and some local plans are also offering it as a no-cost option, increasing the number of people who depend on CNID working.
6. A new generation of CNID signaling allows short text information to be transmitted along with the calling number, so that the recipient can identify the caller even if they have never seen the number before.

In addition, in 20-20 hindsight many of our criticisms seem

overstated. For example, we argued that since CNID doesn't identify the individual, you never really knew who was calling. That's true enough, but do my family and friends care whether it is I or my wife calling to arrange a visit? We argued that a stranded teenager calling from a pay phone might have his call rejected, but would a parent with a teen out on a date really turn down calls from an unknown number?

I think the lesson here is that we need to remember to be humble, and to avoid crying wolf about the RISKS we perceive. Overall, CNID's benefits far outweigh its drawbacks, and we have done society a disservice by encouraging people to block it. We were right to point out the potential weaknesses and incorrect marketing claims, but we erred in encouraging so many people to unnecessarily block their phone numbers, inconveniencing their friends and family while gaining almost no real benefit.

Geoff Kuenning geoff@cs.hmc.edu <http://www.cs.hmc.edu/~geoff/>

✶ Open letter: Why "dot-xxx" is for Chumps

<Lauren Weinstein <pfir@pfir.org>>

Mon, 19 Sep 2005 09:55:28 -0700

This is an open letter addressed to that segment of the Internet community where the *real* money is made -- the "adult entertainment" industry. For

that matter, the operators of the ubiquitous non-commercial sexually-oriented Web sites can join in as well.

I have some free advice that may save you a great deal of grief.

Now, in all honesty, I don't have any particular love for your operations or your products. I'm not a prude (well, not much of one, anyway), but by continuing to push the envelope you folks have engendered a great deal of negative reaction that's approaching a fever pitch.

That reaction is what I'm really concerned about, since it's likely to splatter collateral damage broadly across a wide range of free speech and civil liberties arenas.

So, in my desire to protect them, I'll try to protect you as well.

My advice? Don't fall into the "dot-xxx" trap that's being set for you by ICANN.

As you no doubt are aware, ICANN appears to be preparing for the deployment -- despite broad protests across the political spectrum and a couple of delays -- of a "dot-xxx" top-level domain (TLD).

I've explained elsewhere (<http://www.pfir.org/ip-exexex>) and (<http://www.pfir.org/ip-exexex-01>), why dot-xxx is an absolutely atrocious idea.

ICANN claims that participation in the domain will be voluntary, and that will indeed be the case -- at first.

But as I discussed back in a 2001 PFIR position paper on "domain ghettoization" ([<http://catless.ncl.ac.uk/Risks/24.05.html> \(15 of 22\)2008-01-01 16:36:08](http://www.pfir.org/statements/ghetto-</p></div><div data-bbox=)

[domains](#)), such

efforts are a slippery slope likely leading to widespread filtering and censoring by ISPs, governments, plus a broad range of other entities, affecting a *lot more* than merely pornographic materials. A glance at the current Supreme Court situation is not particularly encouraging in this regard.

ICANN apparently doesn't view their dot-xxx plan as a trap. They seem to consider themselves courageous by pushing on with that TLD despite the broad public and private consensus that it's a terrible concept. Unfortunately, this is the sort of "forge ahead over the cliff" behavior that we've come to expect from ICANN as an organization.

So if dot-xxx arrives, my strong recommendation is that *you ignore it*. Pretend that it doesn't exist. Allow it to be an empty database. Joining that domain won't provide you with any cover -- what you'll actually be doing is painting a giant bulls-eye on yourselves -- and on a vast array of worthy and important groups and materials that have nothing whatever to do with adult entertainment.

Dot-xxx is for chumps.

By the way, I originally considered titling this entry with a domain-related variation on the old "Suppose They Gave a War and Nobody Came" line, but while the situation with dot-xxx is indeed dangerous -- and an example of so much that's wrong with Internet Governance in general and ICANN in

particular -- this matter is anything but a dirty joke.

Lauren Weinstein, lauren@pfir.org <http://www.pfir.org/lauren> 1-818-225-2800
Moderator, PRIVACY Forum - <http://www.vortex.com> <http://daythink.vortex.com>

⚡ Router worms and International Infrastructure

<Gadi Evron <ge@linuxbox.org>>
Fri, 30 Sep 2005 23:29:29 +0200

Michael.Dillon@btradianz.com wrote:

> Reading through the original Russian posting here
> <http://www.securitylab.ru/news/240415.php&direction=re&template=General&cpl=>
> It seems that someone has built an IOS worm that
> follows an EIGRP vector from router to router.

A while back I emailed the following text to a closed mailing list. I figure now that quite a few cats are out of the bag it is time to get more public attention to these issues, as the Bad Guys will very soon start doing just that.

Ciscogate by itself ALONE, and now even just a story about worms for Routers is enough for us to be CLEAR that worms will start coming out. We do learn from history.

So.. as much as people don't like to talk much on the issues involving the so-called "cooler" stuff that can be done with routers, now is the time to start.

Here is one possible and simple vector of attack that I see happening in the future. It goes down-hill from there.

I wrote this after the release of "the three vulnerabilities", a few months back. Now we know one wasn't even just a DDoS, and that changes the picture a bit.

Begin quoted text ----->>>

More on router worms - let's take down the Internet with three public POCs and some open spybot source code.

- - -

People, I have given this some more thought.

Let's forget for a second the fact that these vulnerabilities are dangerous on their own (although it's a DoS), and consider what a worm, could cause.

If the worm used the vulnerability, it would shoot itself in the leg as when network is down, it can't spread.

Now, imagine if a VX-er will use an ancient trick and release the worm, waiting for it to propagate for 2 or 3 days. Then, after that seeding time when the say.. not very successful worm infected only about 30K machines around the world, each infected host will send out 3 "One Packet Killers" as I like to call them to the world.

Even if the packet won't pass one router, that one router, along with thousands of others, will die.

Further, the latest vulnerabilities are not just for Cisco, there is a "One Packer Killer" for Juniper as well.

So, say this isn't a 0-day. Tier-1 and tier-2 ISP's are patched (great mechanism to pass through as these won't filter the packet out if it is headed somewhere else), how many of the rest will be up to date?

Let's give the Internet a lot of credit and say.. 60% (yeah right).

That leaves us with 30% of the Internet dead, and that's really a bad scenario as someone I know would say.

Make each infected system send the one packet spoofed (potentially, not necessarily these vulnerabilities) and it's hell. Make them send it every day, once! And the net will keep dying every day for a while.

As a friend suggested, maybe even fragment the packet, and have it re-assembled at the destination, far-away routers (not sure if that will work).

These are all basic, actually very basic, techniques, and with the source to exploits and worms freely available.... We keep seeing network equipment vulnerabilities coming out, and it is a lot "cooler" to bring down an ISP with one packet rather than with 1,000,000,000,000,000.

I am sure the guys at Cisco gave this some thought, but I don't believe this is getting enough attention generally, and especially not with AV-ers. It should.

This may seem like I am hyping the situation, which is well-known. Still well-known or not, secret or not, it's time we prepared better in a broader scale.

How?

Gadi.

----->>> End quoted text.

I would really like to hear some thoughts from the NANOG community on threats such as the one described above. Let us not get into an argument about 0-days and consider how many routers are actually patched the first... day.. week, month? after a vulnerability is released.

Also, let us consider the ever decreasing vulnerability-2-exploit time of development.

I don't want the above to sound as FUD. My point is not to yell "death of the Internet" but rather to get some people moving on what I believe to be a threat, and considering it on a broader scale is LONG over-due.

The cat is out of the bag, as as much as I avoided using "potentially" and "possibly" above to pass my point.. this is just one possible scenario and I believe we need to start getting prepared to better defending the Internet as an International Infrastructure.

As I am sure that this will be an interesting discussion, I am also sure this will eventually derail to a pointless argument over an unrelated

matter, here on NANOG. I'd appreciate if people who are interested would also email me off-list so that we can see how we can perhaps proceed with some activity.

My blog: <http://blogs.securiteam.com/?author=6>

Wolf Blitzer repeats Rudy in questioning governors (Re: [RISKS-24.04](#))

<Fred Cohen <dr.cohen@mac.com>>

Sun, 18 Sep 2005 09:30:59 -0700

This morning I watched as Wolf Blitzer on CNN questioned governors about preparedness, and the single frequency question came up again - in that form. It just shows how the power of ideas can take on its own life. Fortunately the mayors of Miami and Boston were more clued in than Rudy. Florida indicated that the he believed that the problem was solved there without referring to a single frequency in his response. Boston indicated the use of a system by Raytheon that allows interconnections between different frequency bands for specific emergency communications requirements. Hopefully Wolf will start to ask the right question after he finds out that the notion he is spreading is flawed.

Thanks also to the many people who have responded to me personally with their views -- all reasoned views -- are as always welcomed.

Security Posture <securityposture.com>, Fred Cohen & Associates

<all.net>

572 Leona Drive, Livermore, CA 94550 1-925-454-0171, University
of New Haven



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 6

Wednesday 5 October 2005

Contents

- [Google, Privacy, and Masochism](#)
[Lauren Weinstein](#)
- [Legal docs expose various risks in routine Diebold maintenance in NC](#)
[Joseph Lorenzo Hall](#)
- [Car and van collide](#)
[Kathy Uek via Monty Solomon](#)
- [Y2K glitches linger](#)
[George C. Kaplan](#)
- [Windows delete command can fail silently](#)
[Diomidis Spinellis](#)
- [Buffer overrun in television sets](#)
[Matt Roberds](#)
- [Why telephone "Caller ID" is actually now even worse than we expected](#)
[Lauren Weinstein](#)
- [Re: Mea culpa: How we got it wrong on CNID](#)
[Kelly Bert Manning](#)
- [Windows and USB devices](#)
[Mike Swaim](#)

- [Router worms and International Infrastructure](#)
[Gadi Evron](#)
 - [D.C. Red-Light Cameras Fail to Reduce Accidents](#)
[Monty Solomon](#)
 - [Re: Katrina victims required to use Microsoft IE](#)
[Michael Bacon](#)
 - [Re: Kitten on the keys...](#)
[Andrew Koenig](#)
 - [CCSA Fall Symposium Call for Participation 3 Nov 2005](#)
[Michel Kabay](#)
 - [Info on RISKS \(comp.risks\)](#)
-

🔥 Google, Privacy, and Masochism

<Lauren Weinstein <lauren@vortex.com>>

Tue, 04 Oct 2005 16:24:46 -0700

Today Google and Sun Microsystems announced a joint venture, and while their grand plan seems somewhat murky at this point, there is speculation that their goal is to move toward "hosted" versions of applications (such as Sun's "StarOffice") that would run largely on remote central servers instead of local users' PCs, theoretically allowing access from any Internet location. This would presumably present formidable competition to Microsoft's own software products.

Whether or not this is actually the Google/Sun target, it's worth taking a moment to review where we stand right now regarding Google in some important respects.

Google keeps records of your searches, and can tie them to other

activities
via cookies. Google scans the e-mail you send and receive
through
Gmail. Google collects a variety of information on your other
browsing
activities through various optional toolbars and services.

Google wants to make copies of copyrighted books without paying
for them.
Arguments about how they might make "snippets" of such materials
available
in "Google Print" aside, the internal R&D value alone of that
collection to
Google would presumably be immense, and all without sending a
dime to the
copyright holders.

When CNET ran a story using Google to research data on Google's
chief exec,
Google reacted like an enraged and petulant child.

Now, with the new Sun Micro deal, if hosted versions of word
processing and
related applications are developed and deployed by the joint
Google and Sun
team, Google could quite possibly be tied into your document
editing and
other Office-like activities if you use such services.

Google refuses to hire a privacy officer (after all, they're the
"Trust us
-- First do no evil" company, and they're smarter than everyone
else
about... well... everything, right?)

Google refuses to detail their data retention policies or the
extent to
which they make that growing corpus of data available to outside
entities.

Of course, it's Sun's Scott McNealy who has famously said: "You
have no
privacy, get over it" and who suggested that consumer privacy is

a "red
herring" issue.

Let's face it, the writing isn't only on the wall, it's dripping
off and
collecting in putrid pools on the floor.

"Trust us" is not enough.

Why does Google so strenuously resist at least consulting with
the privacy
community? What have they got to lose if everything they're
doing is on the
up and up? (I'm certainly willing to assume that this is
currently the
case.) Why do they take such a masochistic approach when it
might be
possible with a relatively few changes to let in the fresh air?

Here's my free advice to Google. Pick up the phone and start
talking to
folks who quite possibly might have more experience dealing with
these
issues than you do, and might even be able to help you. I for
one would be
much happier if I could support Google's efforts rather than
having to be
concerned every time they announce a new project.

Hell, my number is listed below. I'd be glad to chat. But I
won't be
holding my breath waiting for their call.

Lauren Weinstein lauren@pfir.org lauren@vortex.com Tel: +1 (818)
225-2800

<http://www.pfir.org/lauren> <http://www.pfir.org> <http://www.eepi.org>

Lauren's Blog: <http://lauren.vortex.com> DayThink: <http://daythink.vortex.com>

Legal docs expose various risks in routine Diebold maintenance in NC

<Joseph Lorenzo Hall <joehall@gmail.com>>

Mon, 3 Oct 2005 23:04:20 -0700

Reference [1] (from Joyce McCloy [of NCVV][2]) is fascinating. It is an exchange between an attorney at Diebold Election Systems, Inc. (DESI) and the general counsel for the North Carolina State Board of Elections. It mostly centers around a few incidents that occurred in Gaston Co., NC. It is a great illustration of a number of worrying characteristics of the vendor/jurisdiction relationship typical of modern election systems.

[1]: <http://www.josephhall.org/nqb2/media/GastonDiebold2004.pdf>

[2]: <http://www.ncvoter.net/>

Three incidents are of particular note:

1. In one city, Dallas, NC, a bug appears to have prevented the downloading of 11,945 votes which wasn't caught for seven days. At which point, it appears the county compared paper print-outs from the precinct with the totals reported by the tabulation server. A DESI technician reproduced the bug twice and then decided to forgo usual DESI protocol and loaded the flash-based memory packs directly into the central (GEMS) server to retrieve the votes from the memory pack.
2. In another case, another memory pack "failed to download" and the DESI technician got approval to send a back-up file electronically

to DESI

technicians who then e-mailed the results back. After writing this data

to a memory pack, the on-site technician loaded them into the central server via a tabulator unit.

3. Finally, the document describes hand-entering of "three to five"

ballots. DESI claims as a "check and balance" this process doesn't allow

the technician to enter more votes than the total vote count (that is,

the number of valid plus spoiled ballots). This would implicate that one

would be prevented from entering more than a certain number of votes,

but, of course, does nothing to constrain what votes are entered. A

human looking over the technician's shoulder is the only other constraint.

I've posted more below the fold:

<http://josephhall.org/nqb2/index.php/2005/10/03/desi_nc>

Joseph Lorenzo Hall, UC Berkeley, SIMS PhD Student

<<http://josephhall.org/>> blog: <<http://josephhall.org/nqb2/>>

Car and van collide

<Monty Solomon <monty@roscom.com>>

Mon, 3 Oct 2005 00:40:50 -0400

Kathy Uek, MetroWest Daily News, 2 Oct 2005

A two-car accident on Rte. 20 in Marlborough in front of Burger King sent

several people to area hospitals, including one who was flown by

medical

helicopter to a Worcester hospital. Police said a handicapped-equipped

two-seat Dodge van was traveling on Rte. 20 when it hit a Lexus traveling in

the opposite direction yesterday at about 11:30 a.m. "The disabled driver's

arm began twitching," said Officer Rob Insani. "Since the controls are on

the steering wheel, he couldn't control the car and it seems like he swerved

into the oncoming lane." ...

<http://www.metrowestdailynews.com/localRegional/view.bg?articleid=110555>

⚡ Y2K glitches linger

<"George C. Kaplan" <gckaplan@ack.berkeley.edu>>

Sat, 1 Oct 2005 16:45:04 -0700

I decided to make a contribution to the Red Cross, so I went to their

website and followed the "Donate by Mail" link. This brings up a simple

form where you can enter your name, address, donation amount, etc, and then

display the info on a page to be printed out and mailed with your check.

On the page I printed, right above my name, is the line:

Today's Date: Saturday, October 1, 105

It appears to be a well-known problem with the Javascript 'getYear()'

method, which is implemented to return either the current year, or (year -

1900), depending on which browser is being used. There are

equally well-known ways to avoid the browser incompatibilities; why the Red Cross doesn't use them is an open question.

George C. Kaplan, Communication & Network Services, University of California
at Berkeley 1-510-643-0496 gckaplan@ack.berkeley.edu

Windows delete command can fail silently

<Diomidis Spinellis <dds@aueb.gr>>
Mon, 03 Oct 2005 16:48:33 +0400

In the Windows XP command interpreter CMD.EXE (the default command line shell) one can specify multiple arguments to the DEL(ete) command, in order to delete multiple files. If at least one of the files can be deleted, the command will not complain about any nonexistent files specified as arguments. For example:

```
C:\> echo.>foo
C:\> del nonexistent foo
C:\> del nonexistent
Could Not Find C:\nonexistent
```

This behavior is non-orthogonal and risky. If one mistypes the name of one of several files that are to be deleted, that file will silently continue to exist. The same will happen if one of the files has the hidden attribute set: DEL will silently ignore it, rather than issue an error message. Although one should not depend on a delete command to reliably obliterate

data, the current behavior can lead to difficult-to-locate bugs, especially in scripts.

Further examination of the command reveals other instances of non-orthogonal behavior. When specifying multiple non-existent files as arguments, DEL will complain only about the first one, but when specifying multiple files with the read-only attribute set, DEL will complain about each one. Also DEL, never sets the ERRORLEVEL environment variable to indicate an error, although other commands, like DIR, set it correctly.

The logic behind a correctly-operating implementation of DEL is trivial.

```
errorlevel = 0
foreach filename
    if not delete(filename) then
        display_error_message(filename)
        errorlevel = 1
    end if
end foreach
exit(errorlevel)
```

If a central and critical piece of the Windows operating system, such as the command shell, can't get the above logic right, what are the chances of having in the system a secure TCP/IP stack, web browser, or firewall?

Diomidis Spinellis - <http://www.spinellis.gr>

Buffer overrun in television sets

<Matt Roberds <mroberds@worldnet.att.net>>

Sat, 01 Oct 2005 00:26:34 +0000

A recent discussion in news:sci.electronics.repair concerned late-model RCA television sets that would suddenly lose their sound. Two repair technicians stated that they could find nothing physically wrong with the sets, and that unplugging the set for a while seemed to cure the problem.

One technician later posted this link:

<http://www.iwaynet.net/~nesda/SilentCTC.html>

According to that article, a device from one particular manufacturer that is used to insert closed captioning and other data into the video stream is generating data that has two bits more than the specification. These two extra bits were causing the microprocessor in the television to become confused. The article claims that Sony, Hitachi, and Philips sets are also affected.

That article is dated June 2001, but the discussion in the newsgroup appears to indicate that this problem has occurred more recently than that.

⚡ Why telephone "Caller ID" is actually now even worse than we expected

<Lauren Weinstein <lauren@vortex.com>>

Sun, 2 Oct 2005 17:33:04 PDT

Recently, a former critic of telephone company "Caller ID

Services" (more properly "Calling Number ID" - CNID) has publicly stated that he has changed his mind and now feels that our concerns (I'm a CNID critic of long standing myself) have turned out to be unjustified.

With all due respect, I must strongly disagree.

First, there's a logical flaw in the argument that simply because one doesn't perceive or experience the sorts of problems cited, that they don't exist -- or that they wouldn't exist even with less or no blocking of CNID. These are both incorrect. In fact, CNID has now become even more dangerous than we ever imagined.

Taking the latter point first, we have no way to know how many problems have been and continue to be avoided by the use of CNID blocking. Most people sensitive to these concerns have been using blocking all along, so by definition to the extent that they're not making non-blockable 800/900-type ANI calls they are relatively protected. Business collection of CNID info may have been somewhat suppressed by the heavy usage of blocking, but if there were less blocking there would almost certainly be more collection since it would become a more valuable resource.

And yet, most of the horror stories still **do** take place. You may not hear about them, but in my role as PRIVACY Forum moderator I frequently get reports that are utterly nightmarish. Spousal abuse facilitated by CNID, massive abuse by businesses that **do** collect the CNID data, and then use it

as an excuse to claim exemptions from the "do not call" lists, and all manner of other problems, some of them life threatening, and particularly bad in regions that don't offer per-line blocking, where one can easily forget to dial the block code on an individual call.

But our crystal ball **was** foggy, in that we never predicted the new CNID scourge that has actually been putting even more lives at risk -- CNID Spoofing. This is becoming very widespread and is being used by crooks, scam artists, stalkers, collection agencies, pranksters, and so on -- and is a total mess. The telcos in general so far can't/won't do anything about this -- it may not be fixable in a practical sense -- and this spoofing is rapidly being commercialized, using PRI telephone trunks and VoIP interfaces. Both CNID number and name info can be easily spoofed in most cases via these systems. It's an enormous problem and getting rapidly worse, and is poised to blow up in a big way in the public sphere, and really give CNID yet another new and very serious black eye.

In a comment to a PRIVACY Forum message in 1993, I suggested that, "As a practical matter, 'spoofing' of caller ID (CNID) systems should not be a significant problem in modern, properly implemented systems."

The last three words in that quote are key. We did not anticipate that untrusted parties would gain routine access to such sensitive aspects of the telephone network in a manner that would allow such abuse.

Lauren Weinstein +1 (818) 225-2800 <http://www.pfir.org> <http://www.eepi.org>

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

Re: Mea culpa: How we got it wrong on CNID (Kuenning, [RISKS-24.05](#))

<bo774@freenet.carleton.ca (Kelly Bert Manning)>

Sun, 02 Oct 2005 22:36:22 -0400 (EDT)

Time out to start. Has Geoff Kuenning done any research about the impact of Caller ID, or is this one of those situations where someone projects their personal experience and assumes that it applies to everyone.

I've been seeing descriptions of the negative consequences of Caller ID for years, including murders, in publications such as Privacy Journal:

<http://www.privacyjournal.net/>

In discussions with people I often notice a gender split. Men tend to think that Privacy is mainly concerned with junk mail, telemarketing and spam, while women tend to assume that it is more to do with not being confronted by someone they wish to have No Contact with.

> Then a few privacy advocates noticed that there was a dark side: if
> you called a local business, it could capture your number with CNID
> and add you to a telemarketing list. Suddenly CNID changed from a
> beneficial service to a nefarious plot.

There is far more to the issue and to the concerns. Caller ID

for a hardline
phone places you at a particular location. That isn't necessarily
the case
for cellular phones, unless someone with access to tower or GPS
data for
that mobile phone can be corrupted. Prepaid cellular solves much
of the
billing data privacy issue. I do agree with Geoff Kuenning's
comments about
cell phones "solving" some Caller ID problems.

> What happened? The answer is simply that I was wrong about
the evils of
> CNID, and wrong about the (perceived lack of) benefits. That
error arose
> primarily from an inability to correctly predict the future.
In particular,
> the following forces have reduced the evils and increased the
benefits:

Privacy Journal sometimes offers prediction about future abuse,
but often PJ
publishes "War Stories" of real life experiences.

> 1. The predicted data collection by small businesses never
happened.

Says who? Is there any researched evidence behind this claim?

Kevin Evans, "President" of the BC Business Council, that is to
say, Paid PR
front man, stated that customers expect businesses to answer the
phone with
"Hello Mr. -politician's surname- are you happy with your Hugo
Boss purchase
from last week?", while making the Business Council's pitch to a
legislative
committee responding to a national mandate to enact private
sector privacy
laws. He made the comment in connection with the issue of Caller
ID, not
ANI.

It is perfectly possible that Mr. Evans was exaggerating the ability and use of Computer Integrated Telephony by business. On the other hand he was making a claim in public and the cost of Computer Integrated Telephony gets cheaper every year. Retrieving a customer name via CNID and associating it with account data and recent purchase history is well within current technology for large, medium or even small businesses. Haven't we seen Risks submissions about companies billing the wrong customer because they use ANI data with the assumption that it uniquely identifies customers?

In my own submission to the legislative committee I responded to Mr. Evan's claim, rhetorically asking how he reconciled it with at least 1/3 of telco customers paying for non published numbers, and with the fact that at least 1/4 of Canadians are Privacy Fundamentalists.

I also changed Evan's scenario to one in which "Mr. Smith's" wife calls a store and is asked "Hello Mr. Smith, are you happy with that gold necklace you bought earlier this week?". I pointed out that Mr. Smith is unlikely to be happy with that, regardless of whether the necklace is a surprise anniversary/birthday gift for his wife, or one for his girlfriend.

> 3. The unforeseen Federal Do-Not-Call List has become an effective defense
> against telemarketing, so revealing your telephone number isn't much of a
> problem anyway.

Again this reflects an idiosyncratic definition and perception of the risks.

The risks of Caller ID are not limited to telemarketing.

A hard line phone number reveals your location at the time you call. Think of the meaning of the phrase "I know where you live". While it has become something of a dramatic cliché it is based on a harsh reality which most people should be able to understand.

There are 100s of millions of people in the world with hard line phones. The fact that Geoff Kuenning hasn't personally experienced a downside of Caller ID doesn't mean that everyone else has been so fortunate.

Most murder victims are killed by someone they know. Personal experiences vary widely and allowance should be made for that. The fact that Geoff Kuenning hasn't been murdered doesn't mean that nobody should worry about homicide.

The display of hard line calling numbers creates a potential for a wide variety of privacy invasion and abuse. Stating that it has never happened seems naive, to say the least.

Personally I found many people using caller ID got confused when the information on my employer paid home phone line was displayed. It can create confusion as well as eliminate it. Eg. I got paged at home and whoever answered my call decided I must be at my office, based on caller ID showing the name of my employer. (My employer provided cell phone was unreliable at home).

⚡ Windows and USB devices (Re: Koenig, [RISKS-24.05](#))

<"Mike Swaim" <mswaim@wotan.mdacc.tmc.edu>>

Sun, 2 Oct 2005 21:54:44 -0500

In [RISKS-24.05](#), Andrew Koenig complains that every time he moves a USB MIDI device to another port, Windows thinks that it's another device. Raymond Chen discusses this behavior in his blog in message <http://blogs.msdn.com/oldnewthing/archive/2004/11/10/255047.aspx>

What is probably happening is that the MIDI device doesn't have a serial number, so Windows can't tell if it's the same device it's seen before or not. So Windows errors on the side of caution and considers it a new device.

Mike Swaim, MD Anderson Dept. of Biostatistics & Applied Mathematics
mpswaim@mdanderson.org or mswaim@odin.mdacc.tmc.edu at work

⚡ Router worms and International Infrastructure

<Gadi Evron <ge@linuxbox.org>>

Sat, 01 Oct 2005 15:49:06 +0200

The subjects of routers security, possible worms and the "taking down of the Internet" are ones that occupy much of my time. Trying to distinguish different threats, plausibility and FUD - as well as finding solutions.

The following is an e-mail message in which I discuss a certain simple scenario to such a risk, and I would really appreciate some feedback on it.

You can find the text in this blog entry:

<http://blogs.securiteam.com/?p=73>

My blog: <http://blogs.securiteam.com/?author=6>

D.C. Red-Light Cameras Fail to Reduce Accidents

<Monty Solomon <monty@roscom.com>>

Tue, 4 Oct 2005 12:43:53 -0400

Del Quentin Wilber and Derek Willis, **The Washington Post**, 4 Oct 2005, A01

The District's red-light cameras have generated more than 500,000 violations and \$32 million in fines over the past six years. City officials credit them with making busy roads safer. But a **Post** analysis of crash statistics shows that the number of accidents has gone up at intersections with the cameras. The increase is the same or worse than at traffic signals without the devices. Three outside traffic specialists independently reviewed the data and said they were surprised by the results. Their conclusion: The cameras do not appear to be making any difference in preventing injuries or collisions. ...

<http://www.washingtonpost.com/wp-dyn/content/article/2005/10/03/>

[AR2005100301844.html](http://catless.ncl.ac.uk/Risks/24.06.html)

⚡ Re: Katrina victims required to use Microsoft IE ([RISKS-24.05](#))

<"Michael \ (Streaky\) Bacon" <himself@streaky-bacon.co.uk>>

Sun, 2 Oct 2005 04:21:06 +0100

Douglas W. Jones wrote about FEMA's website working under one browser (IE) only ... and then not well.

Not too many moons ago, one of the largest oil companies in the world relied upon telex as its stand-by communications system. Rugged, reliable, needing only a telegraph wire to work, reaching multiple audiences, accessible by sophisticated (e.g. PC) devices as well as dedicated telex terminals, working in any language using the Roman alphabet, store-and-forward but with instant access and delivery capability; telex is (was) the epitome of simplicity and availability, practically a guaranteed method of communication in the aftermath of a disaster.

Complex websites, packed with graphics and requiring particular software, fonts, etc. to work properly are not suited to such situations.

The RISKS are manifold, and engineered in by the inability of "imagineers" to truly imagine.

⚡ Re: Kitten on the keys...

<"Andrew Koenig" <ark@acm.org>>

Fri, 30 Sep 2005 22:00:29 -0400

> From: Harvey Fishman
> I read the article in Risks about your contretemps with
regedit and I
> think that the fault here lies with you rather than
Microsoft. I am a
> cat person also, and when I get a new kitten it learns quickly
that
> desktops and computer keyboards are verboten. Water guns are
really
> excellent tools for teaching young cats what is acceptable and
what is
> not. A cat that gets to the age of five months without
learning this
> discipline is the mark of a lazy owner.

The interesting thing is that this particular incident is the
only time I
can recall this kitten actually walking on the keyboard. After
receiving
your e-mail, I watched her normal behavior, which is to jump
from the table
next to my computer stand onto the stand and from there to my
lap, without
touching the keyboard. I have no problem with her behaving that
way.

Anyway, if a kitten can come that close to permanently deleting
a registry
key, so can a dropped object. Such things happen. For that
matter, I
suspect that if I failed to suppress my Unix habits and hit
"delete" instead
of "backspace" at the wrong time, it would have a similar effect.

So what I'm trying to say is that regardless of how my cats
behave, I don't
think it's wise to design a software system that allows a single
keypress to

make an irrevocable change to the system's state.

PS: I don't think using a water pistol near computer equipment is a real good idea, either.

CCSA Fall Symposium Call for Participation 3 Nov 2005

<"Michel Kabay" <mkabay@starband.net>>

Tue, 4 Oct 2005 05:26:13 -0400

The Cyber Conflict Studies Association Fall 2005 Symposium will be held November 3, 2005 in Arlington, VA. The CSC is a non-profit entity organized to promote and lead research and intellectual development efforts to advance the field of cyber conflict.

This Symposium will form the basis for the initial issue of the Cyber Conflict studies Association's *Journal of Cyber Conflict Studies* and will help create agendas for Workshops in the Spring of 2006.

Full details of the conference can be downloaded as a PDF file from

http://www2.norwich.edu/mkabay/unlinked/ccsas_cfp.pdf

The registration form is available from

http://www2.norwich.edu/mkabay/unlinked/ccsas_reg.doc

For further details, contact Jane Swann at <mailto:kswann@norwich.edu >.

M. E. Kabay, PhD, CISSP <http://www2.norwich.edu/mkabay/>

* Assoc. Prof. Info. Assurance * Prog. Dir., MSc & BSc in Info. Assurance

* CTO, Online Graduate Programs

<http://www.msia.norwich.edu/overview.htm> <http://www2.norwich.edu/mkabay/bsia>

Norwich University, Northfield VT V: +1.802.479.7937

mkabay@norwich.edu

* Network World Fusion Security News1 <http://www.nwfusion.com/newsletters/sec>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 7

Thursday 13 October 2005

Contents

- [Takeoff at Logan aborted by errors](#)
[Mac Daniel via Monty Solomon](#)
- [Faulty radar serving Logan leaves thousands stranded](#)
[via Monty Solomon](#)
- [Translation can be hazardous to your identity?](#)
[Mark Brader](#)
- [NOAA's radio transmitters missing backup power](#)
[Danny Burstein](#)
- [The number 7 blocks Belgian ATM machines](#)
[Lindsay Marshall](#)
- [We are from the /Greek/ government and we are here to help. Really!](#)
[Vassilis Prevelakis](#)
- [Risks of Web 2.0, or, the MySpace worm](#)
[Paul Bissex](#)
- [Unusually slick phishing attempt](#)
[Nickee Sanders](#)
- [Re: Airbus, Whistleblower Dispute A380 Pressurization Controls](#)
[Kurt Doppelbauer](#)

- [Re: B777 incident](#)
[Peter B. Ladkin](#)
 - ["One Frequency"](#)
[Jay R. Ashworth](#)
 - [Re: Windows delete command can fail silently](#)
[Joe Loughry](#)
 - [Re: Mea culpa: How we got it wrong on CNID](#)
[Geoff Kuenning](#) [Jon A. Solworth](#)
 - [Criticism of Caller ID Well Founded](#)
[Robert Ellis Smith](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈️ Takeoff at Logan aborted by errors

<Monty Solomon <monty@roscom.com>>

October 7, 2005 12:51:46 AM EDT

An American Airlines jet aborted its takeoff at Logan International Airport on 4 Oct 2005, after errors by a pilot and a controller allowed another plane to cross onto its runway. An FAA spokesman could not say how close the planes had come to colliding, but said the American Airlines flight was rolling at the time its takeoff clearance was canceled. An aviation source familiar with the investigation said the planes came within 1,000 feet. The incident was the second runway incursion in just over a week. On 27 Sep 2005, a FedEx cargo jet that had just started its takeoff came within 2,000 feet of a twin-propeller plane crossing the same runway. The two incidents bring to 16 the number of runway incursions since Oct 2004 at Logan, a number that has alarmed airport and federal officials. ...

[Source: Mac
Daniel, *The Boston Globe*, 6 Oct 2005; PGN-ed]

[http://www.boston.com/news/local/massachusetts/
articles/2005/10/06/takeoff_at_logan_aborted_by_errors/](http://www.boston.com/news/local/massachusetts/articles/2005/10/06/takeoff_at_logan_aborted_by_errors/)

✈ Faulty radar serving Logan leaves thousands stranded

<Monty Solomon <monty@roscom.com>>
Wed, 12 Oct 2005 04:02:45 -0400

Faulty radar serving Logan leaves thousands stranded
Monitors show objects that don't exist; solution uncertain

A malfunctioning radar system serving Logan International
Airport caused
flight cancellations and delays of several hours yesterday,
stranding
thousands of passengers on a holiday weekend and adding to the
woes of an
airport that has logged several runway incidents in the past few
months.

[Source: Donovan Slack, *The Boston Globe*, 11 Oct 2005]
[http://www.boston.com/news/local/articles/2005/10/11/
faulty_radar_serving_logan_leaves_thousands_stranded/](http://www.boston.com/news/local/articles/2005/10/11/faulty_radar_serving_logan_leaves_thousands_stranded/)

[More: Radar malfunction causes long delays at Logan, *The
Boston Globe*, 11
Oct 2005

[http://www.boston.com/news/local/massachusetts/
articles/2005/10/11/
radar_malfunction_causes_long_delays_at_logan/](http://www.boston.com/news/local/massachusetts/articles/2005/10/11/radar_malfunction_causes_long_delays_at_logan/)

Airport travelers play the waiting game, Many in the dark about
radar

glitch, Heather Allen, *The Boston Globe*, 11 Oct 2005]
[http://www.boston.com/news/local/massachusetts/
articles/2005/10/11/airport_travelers_play_the_waiting_game/](http://www.boston.com/news/local/massachusetts/articles/2005/10/11/airport_travelers_play_the_waiting_game/)

]

⚡ Translation can be hazardous to your identity?

<msb@vex.net (Mark Brader)>

Tue, 11 Oct 2005 15:58:28 -0400 (EDT)

As is often done in Europe, the agency operating streetcars in the French city of Grenoble has provided ticket-selling machines that can be operated in more than one language. It was reported this week in uk.transport.london that if you select English, the machines welcome you to London's Croydon Tramlink system! Seen here:

<http://www.ajg41.plus.com/images/rail/fr-grenoble-tramlink02.jpg>

Mark Brader, Toronto, msb@vex.net

[That is positively Grin-noble. I croyd on it. PGN]

⚡ NOAA's radio transmitters missing backup power

<danny burstein <dannyb@panix.com>>

Tue, 11 Oct 2005 13:09:42 -0400

Background: during the power failure two years ago, the NOAA (National Weather Service) radio station serving NYC was dead....

These stations are part of the real emergency network and are supposed to

stay up after anything short of a direct nuclear hit...

NYC recently printed a "what to do in a hurricane" booklet and mentioned tuning into this station, pointing out there were automatic "alert" radios designed for this...., so...

I wrote to NYC's Office of Management describing the outage. They were kind enough to reply. [Excerpts attached]

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

Date: Tue, 11 Oct 2005
From: [snip, an OEM address]

Dear Mr. Burstein,

Thank you for your written correspondence to OEM Commissioner Joseph F.

Bruno, regarding your concerns pertaining to the NOAA All-Hazards Radio.

Commissioner Bruno has asked me to look into this issue for you.

[snip]

[The NOAA contact rep] advises that the NOAA All Hazards Radio has "dual"

transmitters; a primary and secondary. If the primary transmitter fails,

the NWS can utilize the secondary transmitter. However, at this point in

time, the NWS does not have an emergency power backup for the transmitter.

... The NWS has been in contact with the (owners of the transmitter site),

and are awaiting a cost estimate for this service.

[The RISKS are obvious. Readers in other areas of the country, especially those prone to hurricanes/tornadoes/other natural disasters, and who rely

on these stations, might want to check them out as well.]

✶ The number 7 blocks Belgian ATM machines

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

Wed, 12 Oct 2005 15:22:35 +0100

The Dexia Bank ATM machines are experiencing a curious problem. The machines stop functioning when someone enters the number 7, making it impossible for people with a 7 in their pin (personal identification number) code to perform a cash withdrawal.

The problem has been occurring for a month. To prevent people from running out of cash, they are able to perform cash withdrawals inside. "We are experiencing a problem with the software", a Dexia spokesman admitted last wednesday in the daily journal Het Laatste Nieuws, "the problems should be solved within three weeks."

<http://www.nu.nl/news.jsp?n=603834&c=122&rss> (Dutch, 5 Oct 2005)

✶ We are from the /Greek/ government and we are here to help. Really!

<Vassilis PREVELAKIS <vp@drexel.edu>>

Sun, 9 Oct 2005 06:13:34 -0400 (EDT)

The internal revenue service of the Greek ministry of finance is

providing
programs on their web site to help Greek citizens and firms fill-
in
electronic tax forms. The ministry expects everybody with a
computer to
download and run these program as certain tax-forms may only be
submitted
electronically.

I have talked to the people at the ministry and they did not
appear to think
that there is anything wrong with asking everybody to run
programs provided
(only in binary form) by the government.

I asked them if they would consider providing me with the source
of the
programs but they were loath to release it because they were
afraid that
unscrupulous people would modify it and try to sell it (the
programs may be
downloaded for free from the ministry's web site).

When I explained to them my fears that this looks like an
Orwellian
nightmare (cf with the TV sets used in Orwell's 1984 to monitor
citizens),
they were rather surprised saying that nobody has mentioned this
to them
before! (Am I the only paranoid person in Greece?)

Of course, nobody is forced to use the programs, although in
many cases they
save so much time, that it is difficult to convince someone not
to use them
because of some nefarious threat. Once more convenience trumps
security.

Another issue not strictly security related, is that the Greek
government
assumes that everybody uses Microsoft Windows. Some parts of
their web site
refuse to talk to non-Microsoft browsers (they redirect to an

error page),
and the programs they supply run only under Windows.

Conspiracy theorists would surely make something out this, but I strongly believe that the people at the ministry have the best intentions; they simply did not think things through.

The Ministry now plans to provide Java-based programs that should run on non-Microsoft platforms and may make the source code available to academic institutions or non-governmental organizations for auditing purposes.

Still the whole experience shows how easy it is for state agencies to reach out in the homes of their citizens.

Vassilis Prevelakis, Computer Science Department, Drexel University

⚡ Risks of Web 2.0, or, the MySpace worm

<Paul Bissex <pb@e-scribe.com>>

Thu, 13 Oct 2005 15:00:16 -0400

An individual "managed within 24 hours to become the most popular civilian on myspace with the help of a clever bit of viral javascript imbedded into his myspace page... By the time myspace shut down their site for a few hours to investigate he had over 1 million requests from unknowing myspace members for him to be listed as their myspace friend."

Details at:

<http://fast.info/myspace/>

This seems like a new class of XSS, "Level 3" if you will:

<http://e-scribe.com/news/103>

Paul Bissex <pb@e-scribe.com> PO Box 847, Northampton MA 01061
USA

<http://e-scribe.com/> Database-driven web development Open
source software

Unusually slick phishing attempt

<Nickee Sanders <njsanders@ihug.co.nz>>

Thu, 13 Oct 2005 22:07:39 +1300

Whilst clearing out his morning spam collection today, my husband came across an unusually slick phishing attempt. This one's victim-bank is Halifax Bank in the UK. The subject line reads "URGENT ATTENTION - Halifax-Online Fraud Notice" and the body begins by advising of recent phishing attempts against Halifax customers (which, according to Halifax's own site, is even true) and then asks the customer to contact Halifax on receipt of such e-mails!! (The customer service phone number quoted is even the real one.) Extremely cheeky.

The e-mail continues by advising that Halifax has updated their security system. They are proud of their new SSL servers "where there is no risk of fraud and your account details are kept encrypted at all times."

Naturally, because of this update, you are....guess what?.....
asked to log
on to the system and "verify your account info at the following
link"

Such link being of the usual format -- an IP address
(211.35.64.201) hidden
behind a reasonable-looking URL -- which points to a real page
on Halifax's
servers.

The e-mail is unusually slick, as well as being cheeky. It's
almost devoid
of spelling mistakes ("unauthorized" should be "unauthorised"
since it
purports to come from a British company) and likewise of grammar
mistakes
("securer" instead of "more secure" and one missing "to"). It
could easily
have come from a real person at the bank.

The image at the top of the e-mail actually comes from the real
Halifax
servers; as mentioned, the phone number quoted will actually get
you to
Halifax customer service, and if the URL is typed in by hand to
a browser
it will get you to Halifax's own servers.

This phishing attempt is almost perfect, as far as I can see.
Great use of
social engineering. Professionally put together. Very scary.
I give them
a grade of 98% for this project.

Nicke Sanders, Software Engineer, Auckland, New Zealand

[I've seen many of very sophisticated Phishing attacks lately,
purporting
to be BofA, WellsFargo, etc. Some of them take a lot of study
to realize
they are bogus. BEWARE!!!! PGN]

[Airbus, Whistleblower Dispute A380 Pressurization Controls \(R 24 05\)](#)

<Kurt.Doppelbauer@tttech.com>

Tue, 11 Oct 2005 15:57:06 +0200

With respect to [RISKS-24.05](#) and the posting on "Airbus, Whistleblower Dispute A380 Pressurization Controls" I'd like to point out that Mr. Mangan is not a whistleblower. Based on the false claims, TTTech has released the following statement.

Moreover, I am personally disappointed that *LA Times* has published an article with very strong allegations against TTTech without profound technical substance. Stefan Poledna CEO TTTech

TTTech defends against false allegations. These allegations were made by a dismissed former employee one year ago and have been proved to be wrong.

Vienna, Austria -- 6 Oct 2005

Stefan Poledna and Georg Kopetz, members of the executive board of TTTech, a leading provider of technology and products in the field of Time-Triggered Technology, have responded to the false allegations about their components as follows:

1. TTTech's first priorities are safety and adherence to all certification procedures.

2. TTTech is a producer of time-triggered communication systems. Renowned international research institutions and companies have participated in the development of Time-Triggered Technology for more than 25 years. TTTech is considered to be a leading supplier in the field of data communication systems for aircraft and other transportation systems. TTTech's products offer a very high degree of safety. For this reason leading companies have selected this European leading-edge technology. TTTech does not develop cabin pressure control systems.

3. The former employee had been employed by TTTech for six months before his contract was terminated. He made his allegations only after his dismissal on October 1, 2004. A few days before contract termination, he had praised TTTech's achievements for Airbus A380 in an e-mail to the management. This former employee is not a "whistleblower".

4. The allegations made by this former employee have been thoroughly reviewed by TTTech's customers and the authority EASA (the European Aviation Safety Agency). Creating aircraft designs is an iterative process. The TTTech components are certified under the rigors applicable to newly designed aircraft products, thereby assuring safety of flight. The involved companies and authorities issued the following official statement several months ago: "The matters raised by the former TTTech employee have been thoroughly reviewed by TTTech's customers and EASA (the European counterpart to the U.S. Federal Aviation Administration). Creating aircraft

designs is an iterative process. The TTech components will be certified under the rigors applicable to newly designed aircraft products, and safety of flight will be assured."

5. The court repeatedly asked the former employee to substantiate his allegations. But neither in the action for provisional injunction issued by the civil court of Vienna at the end of October 2004 nor in the common trial in court was he able to supply any evidence that would prove failures by TTech, or any safety defects in the components supplied by TTech.

6. The court has never forbidden the former employee from discussing safety issues of TTech products in public. However, the court imposed an order to the former employee not to disclose confidential documents and trade secrets to third parties, nor to make statements that would discredit TTech, such as the allegation that ``TTech participates in a criminal conspiracy.''

see also at:

http://www.ttech.com/press/docs/pressreleases/PR_2005-10-06-TTech-WDR.pdf

Kurt Doppelbauer, TTech Computertechnik AG, Schoenbrunner Strasse 7, A-1040 Vienna, Austria +43 1 585 34 34-18 <http://www.ttech.com>

✈ **Re: B777 incident (Ladkin, [RISKS-24.03](#), Wright, [RISKS-24.05](#))**

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>

Sun, 09 Oct 2005 07:59:37 +0200

For those Risks readers who may not have made the connection, the B777 partial loss of control incident reported by Charles Wright in [RISKS-24.05](#) and that reported by me in [RISKS-24.03](#) are the same incident.

Peter B. Ladkin, University of Bielefeld, Germany
www.rvs.uni-bielefeld.de

⚡ Disaster comms

<Rob Slade <rslade@sprint.ca>>

Wed, 12 Oct 2005 08:26:06 -0800

The Dutch government is testing a warning system that sends text messages to mobile phones during public emergencies. Called 'cell broadcast', the technology will let authorities send messages to all mobile phone users in a specific zone, and will be used in conjunction with other emergency warning systems.

<http://www.smh.com.au/news/breaking/holland-tests-disaster-text-service/2005/10/06/1128562930005.html>

As previously noted, telephone is unreliable in a disaster, and cell service fails almost completely. Private radio may remain up, as long as repeaters or other infrastructure is not required (also think about battery recharging) but there may be contention for bandwidth. However, recent disasters have demonstrated that SMS service tends to remain functional. (However, there are also recent studies that note the ability to DoS the

cell service in its entirety with a flood of SMS traffic.)

rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.
niu.edu

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

✦ "One Frequency" (Re: [RISKS-24.04](#))

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

Sat, 17 Sep 2005 15:16:18 -0400

Clearly, what Rudy Giuliani was incorrectly quoting from his technical advisors who actually *knew* what they were talking about, was the necessity to allocate and provision between other categories of agencies what firefighters have had for years: interagency coordination channels.

Fire fighting has been an inter-jurisdictional issue much longer and more frequently than law enforcement, and so the fire people have simplex frequencies on which they can talk with their compatriots borrowed from other jurisdictions when large fires strike.

There are, though, many other things that caused communications problems during Katrina and it's aftermath (as the communications engineering people who were likely begging for the solutions to these problems for years, but could not get them funded, would likely tell you):

* Trunking radio: While trunking is useful for reducing required

spectrum

for an agency (you can assign "a fraction of" a channel to a given

agency), it relies on the same sort of centralized systems as Nextel's

consumer trunked SMR service currently does, and fails the same way.

* Nextel itself: Nextel is great, but is **not** engineered to the standards

necessary to utilize it in life safety applications (and while they **used**

to say this explicitly, these days what I see from them instead seems to

be **marketing** to those sorts of people). If a major emergency hits,

knocking out municipal power and toppling towers, Nextel's going down too.

* Digital public safety radio: While there is now an interoperable standard

for digital radio (APCO 25), there are many legacy digital public safety

systems, both trunked and not, that are not interoperable.

* Lack of prep: how hard you have to prep (spare battery counts; off-grid

recharging, etc) depends on what you're planning **for**. The levies and

dikes in Holland (much of which is also below sea level) are built for a

4000-year storm. So you can **do** that sort of thing, if you have the

political will.

Short version: just because the politicians don't know how to phrase it

doesn't mean that the technicians in the background don't know what's

necessary. Give them their heads, and some of the US\$200B, and they'll

fix these problems for you.

Ashworth & Associates, St Petersburg FL USA 1 727 647 1274
<http://baylink.pitas.com>

⚡ Re: Windows delete command can fail silently

<"Loughry, Joe" <joe.loughry@lmco.com>>

Wed, 05 Oct 2005 16:00:18 -0600

> The logic behind a correctly-operating implementation of DEL is trivial...

Watch out, though---the way that commands set ERRORLEVEL is *different* from the way that library functions (and system calls) set the value of "errno."

ISO/IEC 9899:TC2 (currently the most up-to-date C Language standard---well...committee draft, anyway) says that "errno" behaves this way:

> *The value of errno is zero at program startup,*
[emphasis added]
> but is never set to zero by any library function.[Note 172]
The value of
> errno may be set to nonzero by a library function call whether or not
> there is an error, provided the use of errno is not documented in the
> description of the function in this International Standard.
>
> 172: Thus, a program that uses errno for error checking should set it to
> zero before a library function call, then inspect it before a subsequent
> library function call. Of course, a library function can save the value
> of errno on entry and then set it to zero, as long as the

original value

> is restored if errno's value is still zero just before the return.

Joe Loughry, Lockheed Martin Trusted Information Systems and Solutions

RADIANT MERCURY, 1-303-971-2951 joe.loughry@lmco.com

Re: Mea culpa: How we got it wrong on CNID (Kuenning, [RISKS-24.05](#))

<Geoff Kuenning <geoff@cs.hmc.edu>>

05 Oct 2005 14:23:45 -0700

Lauren Weinstein and Kelly Bert Manning both take me to task regarding some of the drawbacks of CNID. Kelly Manning states the position best, I think:

> There are 100s of millions of people in the world with hard line phones. The fact that Geoff Kuenning hasn't personally experienced a downside of Caller ID doesn't mean that everyone else has been so fortunate.

True enough, and you will note that I did NOT issue a call for persons with unlisted telephone numbers to be forced to reveal them via CNID. In fact, I support changing ANI so that calls to toll-free lines don't reveal unlisted numbers.

But there's another side to the counterargument: if 100s of millions of people have hard-line phones, and a relatively small percentage

suffer
problems from CNID, were we correct in campaigning vehemently
against the
service? As I recall we actively attempted to keep it from
being deployed
at all in California.

Instead, perhaps we should have done a better job of balancing
the RISKS and
the benefits. Certainly we need to make sure that people with a
legitimate
need to hide from a stalker understand that CNID reveals their
location, and
give them an easy and reliable way to prevent that. (That also
applies to
new GPS-enabled cellphone services such as "find your friend".)
But I would
like to find a balance where an abused spouse's need for safety
doesn't
prevent me from taking advantage of CNID's very real benefits.

Kelly also writes:

> The fact that Geoff Kuenning hasn't been murdered doesn't mean
that nobody
> should worry about homicide.

No, and it also doesn't mean that I should wander around in
disguise for
fear of being murdered by someone I know. Murder and similar
crimes are
scary, but they can also disproportionately color our thinking.

There is also an error of logic here: if a person is killed
after their
location has been identified via CNID, that doesn't prove that
eliminating
CNID would have prevented the murder. Such crimes predated
CNID. Has there
been a statistical study demonstrating a CNID-related increase
in what we
might call "location-related crimes"?

Finally, as I mentioned to Lauren in private e-mail: just because there are implementation flaws in the current version of CNID doesn't make the concept inherently flawed. By that logic, we might as well ban air travel because of the known flaws in some aircraft.

Geoff Kuenning geoff@cs.hmc.edu <http://www.cs.hmc.edu/~geoff/>

Re: Mea culpa: How we got it wrong on CNID (Kuenning, [RISKS-24.05](#))

<"Jon A. Solworth" <solworth@cs.uic.edu>>
Wed, 05 Oct 2005 23:05:58 -0500

I found Geoff Kuenning's retrospective on CNID very interesting. But I disagree with the "mea culpa" bit. I think we, as part of the intellectual community which thinks about and studies these issues, do have an important role to play in public issues. We can identify the risks. We can describe how a particular risk can be reduced. But at the same time, it is fundamentally not our decision on how to balance these risks (since in almost all cases the issues of risks are a tradeoff). We can inform, it is up to society and to each individual to determine the balance.

Jon A. Solworth, Computer Science Dept., University of Illinois at Chicago

✦ Criticism of Caller ID Well Founded (Re: Kuenning, [RISKS-24.05](#))

<"Robert Ellis Smith" <ellis84@rcn.com>>

Tue, 11 Oct 2005 15:46:10 -0400

Telephone customers have some protections from the negative consequences of Caller ID precisely because privacy advocates expended a lot of energy to assure the availability of number-ID blocking and to create a culture of privacy protection within the new technology. We succeeded. We weren't mistaken!

Geoff Kuenning's numbered arguments conflict with each other. Many of us still lead lives in which protecting the identity of our phone numbers from strangers - not to mention marketers - is vital. I believe that automatic rejection of incoming ID-blocked calls is irresponsible to one's family and self. We can't possibly anticipate when a loved one will be in distress, calling us from a stranger's telephone. Automatic blocking disallows such a call from reaching us. Geoff says that a parent with a teenager on the loose at night would be sure to disengage the automatic blocking feature. Maybe so. But how about the next night, when the kid is safely in bed and an aunt or a cousin or a business associate is trying to reach us from a strange phone? The call will not get through.

Geoff's commentary is comparable to saying that Martin Luther King Jr., was wasting his time because African-Americans now have some degree of equal opportunity. How do we think that came about, by magic? The

efforts of
privacy advocates when Caller ID was first introduced make it
possible for
Geoff to blithely proclaim, there's no privacy problem in 2005,
the battling
back in the 1980s wasn't important.

Robert Ellis Smith, Publisher, Privacy Journal, [www.
privacyjournal.net](http://www.privacyjournal.net),
privacyjournal@rcn.com.

Back in the early 90's, U.S. phone companies began rolling out
the service
known as "Caller ID" (really Calling Number ID, or CNID). Early
adopters
were very pleased with the feature; it helped them to avoid
telemarketers
and occasionally to dodge inconvenient friends.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 8

Weds 26 October 2005

Contents

- [Colleges protest call to upgrade online systems](#)
[Sam Dillon / Stephen Labaton](#)
- [Printer steganography](#)
[Mike Musgrove](#)
- [Meso-Mess: German registration office -- Just leave us alone!](#)
[Debora Weber-Wulff](#)
- [Keep your eyes on the road!](#)
[Peter Scott](#)
- [Internet banking risks need fixing](#)
[Monty Solomon](#)
- [Mileage sign errors](#)
[Monty Solomon](#)
- [OARS privacy problems](#)
[Nanette Asimov](#)
- [Membership database from bankrupt User Group to go to highest bidder](#)
[Dale E. Coy](#)
- [BlackBerry Thumb](#)
[PGN](#)

- [Woman summoned to court over unread Oyster card](#)
[Nick Rothwell](#)
 - [Cingular says: "No password needed" is a Good Thing!](#)
[Steve Fenwick](#)
 - [How ATM fraud nearly brought down British banking: phantom withdrawals](#)
[Andrew King](#)
 - [ACM e-mail looks like Phishing -- again!](#)
[James Garrison](#)
 - [UK electoral registration security issues](#)
[Mike Williams](#)
 - [Interest Earned at a bank not the same as Interest Paid](#)
[Keith Price](#)
 - [Criticism of CNID well founded](#)
[Robert Ellis Smith](#)
 - [Re: Windows delete command can fail silently](#)
[Erling Kristiansen](#)
 - [CFP: Human-Computer Interaction in Aeronautics](#)
[Chris Johnson](#)
 - [Mark Stamp, Information Security: Principles and Practice](#)
[PGN](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Colleges Protest Call to Upgrade Online Systems

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

Sat, 22 Oct 2005 15:52:27 PDT

The federal government, vastly extending the reach of an 11-year-old law, is requiring hundreds of universities, online communications companies and cities to overhaul their Internet computer networks to make it easier for law enforcement authorities to monitor e-mail and other online communications. The action, which the government says is intended to help

catch terrorists and other criminals, has unleashed protests and the threat of lawsuits from universities, which argue that it will cost them at least \$7 billion while doing little to apprehend lawbreakers. Because the government would have to win court orders before undertaking surveillance, the universities are not raising civil liberties issues.

The order, issued by the Federal Communications Commission in August and first published in the Federal Register last week, extends the provisions of a 1994 wiretap law not only to universities, but also to libraries, airports providing wireless service and commercial Internet access providers. It also applies to municipalities that provide Internet access to residents, be they rural towns or cities like Philadelphia and San Francisco, which have plans to build their own Net access networks. So far, however, universities have been most vocal in their opposition.

The 1994 law, the Communications Assistance for Law Enforcement Act, requires telephone carriers to engineer their switching systems at their own cost so that federal agents can obtain easy surveillance access. ...

[Source: Sam Dillon and Stephen Labaton, *The New York Times*, 23 Oct 2005; PGN-ed]

<http://www.nytimes.com/2005/10/23/technology/23college.html?ex=1287720000&en=36556cd12f8fc287&ei=5090>

Printer steganography (Mike Musgrove)

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

Fri, 21 Oct 2005 9:53:05 PDT

Many color printers (Xerox, HP, etc.) add barely visible yellow dots that encode printer serial numbers and time stamps (down to the minute). Intended primarily to combat counterfeiters, the purportedly "secret" steganographic code in color printer copies has now been decoded by four people at the Electronic Frontier Foundation. (The encoding is straightforward, and includes no encryption.) There are of course various slippery-slope privacy issues. [Source: Mike Musgrove, Sleuths Crack Tracking Code Discovered in Color Printers, *The Washington Post*, 19 Oct 2005, D01; PGN-ed]
<http://www.washingtonpost.com/wp-dyn/content/article/2005/10/18/AR2005101801663.html>

[Also noted by Amos Shapir, who suggests you look at the eff site, which nicely documents the encoding:
<http://www.eff.org/Privacy/printers/docucolor/>
PGN]

⚡ Meso-Mess: German registration office -- Just leave us alone!

<Debora Weber-Wulff <D.Weber-Wulff@fhtw-berlin.de>>

Sat, 15 Oct 2005 17:34:04 +0200

The Berlin daily newspaper "Tagesspiegel" has reported on the newest software chaos in town [we actually have a number to contend

with at the
moment... -- dww]:

<http://archiv.tagesspiegel.de/archiv/13.10.2005/2112250.asp>

<http://archiv.tagesspiegel.de/archiv/15.10.2005/2117152.asp>

It seems the registration offices bought themselves some brand-spanking-new software. All people living in Germany must register their address and the names of people who live with them with this office (which is part of the police jurisdiction) inside of a week of moving into town. The police use the data for all sorts of purposes.

They cut over to the new system October 4, and the police suddenly discovered that they were offline - their systems did not work anymore, probably because the API was different. The police had to set up emergency computers directly linked to the official system and have police officers in the field *call in* their requests. Result: the line is always busy. But of course, there is no threat to the general public, just nasty waiting for the police [so maybe they don't need it at all? --dww].

The registration office was pointing the finger at the police, saying they had known for a year that this was coming. Then people called the papers complaining that waiting times at the office - which also issues passports and ID cards and the like - had gone from an hour to FOUR hours.

The official excuse is that clerks were not sufficiently trained in the use of the 23 million Euro software called "Meso". And they insist that the waiting time is "only" doubled, not more. They request the good taxpayers

who paid for the software to just stay home and not bother them until they get the kinks worked out - really, one office gave out a press release to just leave them alone!

An added problem is that many people are trying to apply for new passports because from December on people have to pay more for them because they have to have RFID chips with biometric data stored in them so that the US government is appeased and will still let Germans in without visas.....

Prof. Dr. Debora Weber-Wulff, FHTW Berlin, Internationale Medieninformatik
10313 Berlin <http://www.f4.fhtw-berlin.de/people/weberwu/> +49-30-5019-2320

Keep your eyes on the road!

<Peter Scott <risks@PSDT.com>>
Tue, 18 Oct 2005 10:39:00 -0700

An item in an Information Week article
(<http://www.informationweek.com/story/showArticle.jhtml?articleID=170702055>

: "Car Smarts") brings new meaning to the admonition to keep your eyes on the road:

Toyota is testing technology meant to keep a driver's eyes on the road, according to The Associated Press. The technology employs a camera attached near the car's steering wheel and image-processing software that

recognizes when the driver isn't facing forward. The system flashes a light on the dashboard and beeps when the driver looks away, according to the AP. If the driver doesn't respond, *the brakes are applied automatically*. The feature will be in Lexus luxury models to be sold in Japan next spring.

(my emphasis). Well, *that* sounds reliable... I feel safer already.

I hope they paint them a distinctive color so I can recognize them on the road and stay well away...

⚡ Internet banking risks need fixing

<Monty Solomon <monty@roscom.com>>

Wed, 19 Oct 2005 00:56:32 -0400

Federal regulators will require banks to strengthen security for Internet customers through authentication that goes beyond mere user names and passwords, which have become too easy for criminals to exploit. Bank Web sites are expected to adopt some form of "two-factor" authentication by the end of 2006, regulators with the Federal Financial Institutions Examination Council said in a letter to banks last week. [...] [Source: Feds Want Banks to Strengthen Web Log-Ons, AP item, 18 Oct 2005; PGN-ed] <http://finance.lycos.com/home/news/story.asp?story=52442651>

✶ Mileage sign errors

<Monty Solomon <monty@roscom.com>>

Mon, 17 Oct 2005 02:22:00 -0400

Excerpt from

http://www.boston.com/news/local/articles/2005/10/16/state_rejects_somerville_i_93_lane_shift/

We finally have an answer about how those new state mileage signs got so terribly messed up. And the blame is being placed on Bill Gates. MassHighway admitted that the state had found 19 legends on the new signs with significant errors in mileage. That's 12 percent of the 164 new signs in the \$1.05 million contract.

According to the contractor, some of the distances were calculated using Microsoft's Streets & Trips software. According to Microsoft, the software without a GPS hookup costs \$39.95. This contractor was paid \$130,000 by the state.

Apparently the contractor had tried to use Mapquest, but found it unreliable.

- - - -

Excerpt from

http://www.boston.com/news/local/articles/2005/09/25/in_chelsea_pedalers_celebrate_the_bus/

One sign on Interstate 93 north, near Exit 45 in Andover, reported that Manchester, N.H. was 42 miles away, although the actual distance is just a bit more than 28 miles. Another sign on Route 128/95 in Needham

reported
that Wellesley is 7 miles away. The actual distance is slightly
less than 3
miles. A sign on Route 3 north in Braintree listed the distance
to I-93 as 5
miles when the distance by odometer was 3 miles.

[Also reported by Mark Lutton. PGN]

⚡ Privacy problems

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

Fri, 21 Oct 2005 9:46:07 PDT

San Francisco administrators of OARS, Online Assessment
Reporting System,
issued a generic password (same for all teachers) that left the
system wide
open to anyone who knew a teacher's user name, because many
teachers had not
gotten around to changing the password. [Source: Nanette
Asimov, *San
Francisco Chronicle*, 21 Oct 2005, B2; PGN-ed]

Cingular moved its voicemail system over to an AT&T wireless
service over
the past two weeks. Anyone initializing the account before the
legitimate
owner can then gain total access to the account. Approximately
26 million
Cingular subscribers of the old system are potentially
affected. [Source:
Ryan Kim, *San Francisco Chronicle*, 21 Oct 2005, C1; PGN-ed]

⚡ Membership database from bankrupt User Group to go to highest bidder

<"Dale E. Coy" <dale@thecoys.net>>

Thu, 13 Oct 2005 20:12:39 -0600

http://www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,105386,00.html?source=NLT_PM&nid=105386

Interex membership list for sale to highest bidder; The bankrupt user group's member database is being sold to satisfy creditor demands

A California bankruptcy court will sell Interex's membership database to the highest bidder to help satisfy creditor demands of the bankrupt user group, according to recently filed court papers. The Hewlett-Packard Co. user group claimed about 100,000 members before filing in August for bankruptcy in U.S. Bankruptcy Court for the Northern District of California after incurring more than \$4 million in debt. The court filing is dated Oct. 5, but notices of the sale apparently reached some Interex members this week.

⚡ BlackBerry Thumb

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

Fri, 21 Oct 2005 9:47:39 PDT

Repetitive motion injuries are now entering the mobile handheld world, with doctors reporting a spate of complaints about BlackBerry Thumb.

[AP item seen in the (Palo Alto) *Daily News*, 21 Oct 2005; PGN-ed]

Woman summoned to court over unread Oyster card

<Nick Rothwell <nick@cassiel.com>>
20 Oct 2005 17:06:20 -0000

A woman is being summoned to court, and faces a 1000-pound fine if found guilty, over non-payment of a 1.20-pound London bus fare.

Most of London's transport system is moving over to the Oyster card system, where quasi-smartcards are touched against readers at tube station barriers or doors to buses. A card can contain season tickets, top-up funds for pay-as-you-go travel, or both.

According to the television news coverage today, Jo Cahill believed that she had paid on entering the bus, but the reader did not register her card in order to deduct the fare from the top-up funds. An inspector has treated her as a fare-dodger, even though she explained the situation and offered to pay.

This seems to set the precedent that users are required to confirm that the reader has indeed registered their card, even though the visual and audible signals are not always clear. Transport for London claims that its Oyster card readers rarely fail, although they do not specify whether or not users

will always be taken to court when they do fail. (I frequently get onto buses where the reader has a post-it note saying "reader broken" stuck to it.)

More at: <http://news.bbc.co.uk/1/hi/england/london/4361286.stm>

nick rothwell -- composition, systems, performance -- <http://www.cassiel.com>

✶ Cingular says: "No password needed" is a Good Thing!

<Steve Fenwick <risky_business@w0x0f.com>>

Sat, 15 Oct 2005 17:28:47 -0700

Effective 26 Oct 2005, Cingular is switching to a new voicemail system for all its customers. One of the "features" is "Skip Password"-- apparently, one will no longer need to enter a password if one has physical access to a handset. The option to continue to use a password will still be available, but "skip password" appears to be the default.

>From their website (<http://cingular.com/voicemail_west>):

> Skip Password

> Save time accessing Voice Mail from your wireless handset. Just a one-time

> password setupthat's it. Press and hold 1 from your wireless handset to go

> straight to your voice mail. When accessing your voice mail from another

> phone, your password will be required.

>

> To require a password for all calls from the Main Menu,

> 1) Press 4 for Personal Options 2) Press 2 for
Administrative Options 3)
> Press 1 for Password and follow instructions to turn on your
password

The risks are obvious--to everyone except decision-makers at
Cingular.

⚡ How ATM fraud nearly brought down British banking: phantom withdrawals

<Andrew King <ak-a@ak-a.com>>
Fri, 21 Oct 2005 13:11:57 +0100

Posted on *The Register*

http://www.theregister.co.uk/2005/10/21/phantoms_and_rogues/
with some background at
<http://www.cl.cam.ac.uk/~mkb23/phantom/>

Interesting stuff on risks and responsibilities.

⚡ ACM e-mail looks like Phishing -- again!

<James Garrison <jhg@athensgroup.com>>
Tue, 18 Oct 2005 15:08:08 -0500

The organizations that should know better just don't seem to be
learning.

Today I received a request to participate in a survey, titled
"New ACM
Products/Services Survey" (I am a member of ACM). There were a
number of
things wrong with it:

- 1) The "From" address was not an acm.org address.
- 2) The link to the survey pointed to a site also not in acm.org
- 3) The survey link included an opaque token
- 4) The message was not digitally signed

The fact that the from address and link don't point back to acm.org is a classic hallmark of phishing. The fact that the link contained an opaque token marks it as possible e-mail address harvesting. The lack of a signature means it's not possible to validate the message's authenticity.

Actually, come to think of it, items 1 & 2 may ironically point to the message's authenticity. A real phisher would have made sure the reply-to address and displayed link were in acm.org. So this is either genuine or a very incompetent phisher :-)

Unfortunately, this is the third such e-mail I've received from the ACM in the past couple of years. Each time I point out the obvious problems, and get a polite, if miffed-sounding reply. And nothing changes. How hard is it to buy a copy of PGP (or install GPG) and publish a key for this purpose on the ACM's website?

Of all organizations in the world, I would hope that ACM would be leading the battle against e-mail fraud by example, not lagging far behind. Yes, I know key management isn't simple, but you'd think it would be worth the effort for the ACM.

James Garrison, Athens Group, Inc. 5608 Parkcrest Dr Austin, TX 78731

<http://www.athensgroup.com> 1-512-345-0600 x150 jhg@athensgroup.com

🔥 UK electoral registration security issues

<Mike Williams <mike.williams@globalgraphics.com>>

Fri, 21 Oct 2005 09:19:40 +0100

It is that time of the year in the UK when the annual canvass of electors is done. My form came through the post yesterday. Originally the form had to be completed and returned in the post. A couple of years ago they started allowing you to register by phone, and this year you can now do it via the Internet.

To register by phone or Internet there is a 10-digit reference number on the form. This is that is needed to update the register details by phone (usual automated answering service with 'press key n' to navigate responses). For registering via the Internet there is a 8-letter password.

The reference number and password looks reasonably unguessable - no obvious patterns in the number and the password, although all lower case letters, contains no words. On the down side, all the information is on a single sheet, which as I said was sent through the post. What extra security does the password provide?

The real problem is that the envelope in which the form is sent is the one

that is used to return the form in if it is to be returned, I suppose to try and save some money. Since the envelope is one you have to lick to seal, the registration form was delivered in an envelope that was open!

Interest Earned at a bank not the same as Interest Paid

<Keith Price <price@usc.edu>>

Thu, 20 Oct 2005 10:52:30 -0700 (PDT)

Last month while going over the statement for the one of our interest paying checking accounts from a major bank (one named for a western state that promotes its customer service in ads) I noticed a small discrepancy. The statement (which has recently been redesigned) has an entry for "Interest Earned" and a second one for "Interest Paid." The logical assumption is that you would be paid what you earned. But, this is not the case. Often (at least from recent experience) these differ by \$0.01. In the first instance, the interest earned was \$0.01 more than the interest paid. After noticing this, I had an interesting visit at the near-by branch, which occupied the branch manager for about 45 minutes while he discussed the issue with the people who should know what is happening ("the back office"). He was unable to relay a satisfactory explanation, other than that the 2 numbers come from 2 different systems, that over time it will even out, and that the operations people do not consider this an open problem (there was a strong

indication that they had never heard of this problem). The next month the situation for this account was reversed, i.e. interest earned was \$0.01 less than interest paid, so, at least so far, it has evened out.

How common is this? We have a total of 3 checking accounts at this bank and in the past 2 months have seen this discrepancy 3 times (the 2 times on one account described above, and in the second month on another account). The first occurrence caused me to look through old statements more carefully, but I found no earlier cases.

The risks: Inconsistent treatment of rounding and providing the customer inconsistent information.

✦ Criticism of CNID well founded (Re: Kuenning, [RISKS-24.05](#))

<"Robert Ellis Smith" <ellis84@rcn.com>>

Tue, 11 Oct 2005 15:46:10 -0400

Telephone customers have some protections from the negative consequences of Caller ID precisely because privacy advocates expended a lot of energy to assure the availability of number-ID blocking and to create a culture of privacy protection within the new technology. We succeeded. We weren't mistaken!

Geoff Kuenning's numbered arguments conflict with each other. Many of us still lead lives in which protecting the identity of our phone

numbers from strangers - not to mention marketers - is vital. I believe that automatic rejection of incoming ID-blocked calls is irresponsible to one's family and self. We can't possibly anticipate when a loved one will be in distress, calling us from a stranger's telephone. Automatic blocking disallows such a call from reaching us. Geoff says that a parent with a teenager on the loose at night would be sure to disengage the automatic blocking feature. Maybe so. But how about the next night, when the kid is safely in bed and an aunt or a cousin or a business associate is trying to reach us from a strange phone? The call will not get through.

Geoff's commentary is comparable to saying that Martin Luther King Jr., was wasting his time because African-Americans now have some degree of equal opportunity. How do we think that came about, by magic? The efforts of privacy advocates when Caller ID was first introduced make it possible for Geoff to blithely proclaim, there's no privacy problem in 2005, the battling back in the 1980s wasn't important.

Robert Ellis Smith, Publisher, Privacy Journal
www.privacyjournal.net, privacyjournal@rcn.com.

⚡ **Re: Windows delete command can fail silently ([RISKS-24.06,07](#))**

<Erling Kristiansen <erling.kristiansen@xs4all.nl>>
Sun, 23 Oct 2005 17:17:29 +0200

Windows may also delete the wrong file.

I had two files on a network drive, hosted via Samba on a UNIX server, whose names differed only by capitalization of some letters. Windows Explorer faithfully displayed both names, with the proper capitalization. But when asked to delete one file, it deleted the other one. No warning about a potential conflict was given.

I think this goes back to the half-hearted use by Windows of lower and upper case letters in file names. In some contexts, they are taken to be equivalent, in other cases they are considered different.

I don't know whether this specific problem was due to Windows or Samba. But the end result was rather scary. Luckily, in this particular case, I noticed the problem right away, and was able to re-create the lost file by re-running the application that created it.

CfP: Human-Computer Interaction in Aeronautics

<"Chris Johnson" <johnson@dcs.gla.ac.uk>>

Thu, 20 Oct 2005 16:35:44 +0100

Organized by The European Institute of Cognitive Sciences and Engineering

In cooperation with ACM's Special Interest Group for Computer-Human

Interaction (SIGCHI)

Call for Papers

The international aviation community is advocating goals that compel radical innovation in approach to the fundamentals of aeronautical operations. The role of Human-Computer Integration professionals is to contribute and participate in an active manner to the success of innovation. HCI-Aero 2006 seeks to gather experts and novices from industry, government and academia in the field of human factors in aerospace computing systems. We invite researchers and practitioners to present innovative methods, techniques, tools, and technology. These include air and ground operations, training, design, certification and support both in civil and military applications with a focus on safety challenges, cost effectiveness, performance and comfort. The theme of HCI-Aero 2006 is "Innovation of Aeronautical Operations". This innovation vision finds expression in international air traffic management, coordinated via a satellite-based information exchange, based on coordinated air-ground operations, 4-D trajectory control and reduced constraint in control of aircraft movement. Innovation asserts new modes of operation and technological requirements. These technologies fundamentally change aviation work processes. These advancements impact information redistribution, interactions among agents, decision-making and various optimization processes. The changes in the work of air transportation operations require an approach to research and analysis that includes concern for the changes in the cognitive processes that supports the work in context. =20 Florence Reuzeau and Kevin Corker, General

Co-Chairs of HCI-Aero'06 Dea =20 Submission Deadlines: 15th
March 2006 -

Full Research Papers 15 April 2006 - Industry Papers and Early
Stage

Research Papers=20 15 April 2006 - Panels, Workshops, Posters
and Demos

For more information see the attached call for details or access
the
conference web site on: <http://www.eurisco.org/hci-aero2006>

Mark Stamp, Information Security: Principles and Practice

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

Wed, 26 Oct 2005 10:57:13 PDT

Mark Stamp

Information Security: Principles and Practice

John Wiley (Wiley Interscience), Hoboken NJ

2006

xxi+390

In his preface, Mark Stamp says that he hates black boxes and that the book is intended to illuminate some of the currently popular black boxes. This book seems quite useful as a textbook, with four main thrusts: cryptography, access control, protocols, and software. It includes some challenging problems at the end of each chapter, some of which are quite specific while others are open-ended and thought provoking. Security is of course a huge problem area and difficult to circumscribe. Although this book does not attempt to delve into all of the primary historical paths taken thus far

(for example, understanding the bad ones can be very useful), it does a good job of analyzing where we are today in the areas that it carves out.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 9

Thursday 17 November 2005

Contents

- [Berlin tunnel control fail-safe fails for good](#)
[Debora Weber-Wulff](#)
- [Software bug crashes Japanese stock exchange](#)
[Mark M Bennison](#)
- [Flight Booking System Can't Recognise February 29](#)
[Chris Brady](#)
- [Fun with Daylight Saving Time](#)
[William Reitwiesner](#)
- [Computer Glitch Lets Prisoners Out Early](#)
[Craig S. Bell](#)
- [Radio signal keeps gates and garage doors closed](#)
[Bob Heuman](#)
- [T-mobile erratic behavior](#)
[M. Barnabas Luntzel](#)
- [Freddie Mac profits misstated due to software error](#)
[Jeremy Epstein](#)
- [Some Fast Lane accounts double-billed](#)
[Mac Daniel via Monty Solomon](#)

- [Sony CD DRM Blow-Up Continues -- Recalls Ordered, Lawsuits Possible](#)
[Lauren Weinstein](#)
 - [GPS tracking with Google Maps](#)
[Monty Solomon](#)
 - ['Splogs' Roil Web, and Some Blame Google](#)
[David Kesmodel via Monty Solomon](#)
 - [Whither Goes Google?](#)
[Lauren Weinstein](#)
 - [Amex Blue Chip magic!](#)
[Lindsay Marshall](#)
 - [UK Police Vehicle Movement Database](#)
[Alan Fitch](#)
 - [My approach to CLID / 'phone number privacy issues](#)
[Paul Wexelblat](#)
 - [Re: Cingular: "No password needed" ...](#)
[Kevin Kadow](#)
 - [Two books of possible interest](#)
[PGN](#)
 - [Info on RISKS \(comp.risks\)](#)
-

Berlin tunnel control fail-safe fails for good

<Debora Weber-Wulff <D.Weber-Wulff@fhtw-berlin.de>>

Wed, 09 Nov 2005 08:34:21 +0100

The Berlin daily newspaper "Tagesspiegel" reports on the reason for a massive traffic jam during rush hour on the morning of Nov. 8, 2005:

<http://archiv.tagesspiegel.de/archiv/09.11.2005/2163080.asp>

After a night of repairs to one of the autobahn tunnels in Berlin the crew wanted to test the fire alarm system. They tried starting some of the fire

alarms, and were worried that the automatic gates that are to keep cars from entering a tunnel with a possible fire weren't closing right. They punched more and more alarms, and the gates on both tunnel tubes (work was going on in only one tube) suddenly banged closed - and the computer regulating them crashed.

The gates failed safe - but they couldn't be opened again. Not by hand, and not by computer, which just refused to start again. They worked feverishly from 5am to 10am, trying to get the gates open again so that traffic (which is normally very heavy at that time of the morning), could move. [I'm glad I took the train yesterday! -dww]

Police were able to evacuate cars trapped in the tunnel by way of an exit from the tunnel, which was not gated.

A special complication was that the gates on the north end of the tunnel were made by a different company than the gates on the south end of the tunnel, this caused "additional problems". Which ones, are left to the comp.risks readers as an exercise.

It is still not clear how the error happened or why the computer would not re-start, speculation has it that the computer couldn't handle so many fire alarms at the same time.

Moral of the story:

- * It was good that the system failed safe.
- * It was bad that it did not seem able to handle the number of fire alarms

that are installed in the tubes.

* If you have different suppliers for parts, you want to make sure they are still delivering the same stuff.

Prof. Dr. Debora Weber-Wulff, FHTW Berlin, Treskowallee 8, 10313 Berlin

<http://www.f4.fhtw-berlin.de/people/weberwu/> +49-30-5019-2320
InternatMedieninf

Software bug crashes Japanese stock exchange

<"Bennison, Mark M" <mark.m.bennison@mbda.co.uk>>

Thu, 03 Nov 2005 07:51:21 +0000

"The Tokyo Stock Exchange suffered its worst ever outage yesterday when trading was suspended for four and a half hours due to a software problem.

A spokesman said that the glitch appeared to be connected to the decision to

expand the trading system's capacity last month in response to high trading

volumes. The modified system had worked well, but crashed when the

automatic monthly clean-up of the software was implemented. A back-up system

also failed because it uses the same software."

<http://www.vnunet.com/vnunet/news/2145336/software-bug-crashes-japanese>

Mark Bennison MBCS CITP

Flight Booking System Can't Recognise February 29

<Chris Brady <chrisjbrady@yahoo.com>>

Thu, 17 Nov 2005 11:49:56 +0000 (GMT)

In a Q&A session about our airline's new staff travel online booking system, the following was asked:

Q. I am unable to book [a flight] online because my date of joining is February 29. What should I do?

A. Because you joined in a leap year the system is unable to identify your date of joining. You will need to ask Employee Services to change your date to February 28 for staff travel purposes.

The risk: if the booking system doesn't recognise February 29 then there are going to be a lot of empty flights on that date!! In this post-Y2K age, it is astonishing that we are still suffering from such date issues and this is not even with legacy systems, but brand new ones.

✶ Fun with Daylight Saving Time

<William Reitwiesner <wmaddams@gmail.com>>

Thu, 27 Oct 2005 09:29:40 -0400

The proposed modification to Daylight Saving Time (DST) mentioned in [RISKS-23.94](#) has occurred. The US Congress enacted the Energy Policy Act of 2005 (Public Law 109-58), so starting in 2007 DST in the US will no longer run from the first Sunday in April to the last Sunday in

October, but instead will run from the second Sunday in March to the first Sunday in November. An added benefit is that after the change is implemented, Congress retains the right to undo the change and revert back to the 2005 DST schedules. See Report RS22284 from the Congressional Research Service, available at "<http://www.opencrs.com/document/RS22284/>" and "<http://www.bna.com/webwatch/daylightsavings.pdf>" and elsewhere, for more details.

One wonders how well the embedded time-aware code in most electronic equipment will handle this.

⚡ Computer Glitch Lets Prisoners Out Early

<"Craig S. Bell" <craig_s_bell@yahoo.com>>
Mon, 24 Oct 2005 15:07:47 -0700 (PDT)

Some prisoners were also let out too late, which is just as bad:

<http://www.wlns.com/Global/story.asp?S=4004197>

⚡ Radio signal keeps gates and garage doors closed

<RsH <rsh@idirect.com>>
Fri, 04 Nov 2005 21:36:24 -0500

Apparently garage doors and embassy gates are refusing to work because

something in Ottawa is broadcasting on their radio controlled opener devices' frequencies and swamping them. No one seems to know who/ what is doing it and some fingers point to the military use of that same frequency. The article from the CBC is at the URL below, and is also copied below it. This is, of course, a common problem as we run out of available radio bandwidth and try to cram more and more users into limited space. There is a possibility that the U.S. Embassy or the U.S. military stationed at the Embassy is responsible. Time will eventually tell.

R. S. (Bob) Heuman

<http://www.cbc.ca/story/canada/national/2005/11/04/ottawa-signals051104.html>

Mystery signal blocking Ottawa door devices
Last Updated Fri, 04 Nov 2005 09:37:24 EST
CBC News

Many automatic garage doors in Ottawa have suddenly, and strangely, stopped working, due to a powerful radio signal that appears to be interfering with the remote controls that open them.

J.P. Cleroux of Ram Overhead Door Systems says the phenomenon began last weekend.

"It affects a 25-mile radius. That's huge," said Cleroux.

Angolan Ambassador Miguel Puna's operation is one of those affected by the problem. He can no longer open his embassy's electronic gate.

"Not only in this gate, but even other gates, we are having a lot of

problems," said Puna. "This could cause security concerns."

Two companies that have plotted the reported problems on maps say they appear to cluster in the Byward Market area just east of Parliament Hill, and a corridor leading southeast from there.

The Door Doctor has received more than 100 calls from irate customers who can't operate their doors using the usual remotes.

The company installs and services Liftmasters, the most popular door opener in North America, which operates by radio frequency.

The signal is transmitted on the 390-megahertz band, which is used by virtually all garage door openers on the continent.

That's the same frequency used by the U.S. military's new state-of-the-art Land Mobile Radio System.

Cleroux said operators have already been warned of this phenomenon by service updates from U.S. manufacturers, who started seeing the same problem around military bases last summer. The strong radio signals on the 390-megahertz band simply overpower the garage door openers.

One technician likened it to a whisper competing with a yell.

"From what we hear, it is the American Embassy that's operating on 390, and they're the only ones who can block it. But I'm not 100 per cent sure, because we're all kind of up in the air until we know exactly what's going on," said Cleroux.

The U.S. Embassy denies any transmissions on that frequency. So does the Canadian military.

T-mobile erratic behavior

<"M. Barnabas Luntzel" <mark@luntzel.com>>

Tue, 1 Nov 2005 11:30:37 -0800

The t-mobile sidekick2 has the voicemail number hard-coded, so all I see is "voice mail". Last night, I checked it. It rings. (It isn't supposed to ring.) Someone answers. (Someone isn't supposed to answer.) I say "hmm. this is weird" to the lady. She says "what number are you trying to call?" I say, "well, I don't know!"

So I decide then to call the support number, also built-in as "611". Someone else (not a t-mobile support jockey) answers "Hello?" It sounds similar to the woman I had just called so I ask "did I just call you a minute ago?" she says no. So I say, naturally, "is your number 611?" she says no.

At this point I want to call my mother, to see if it was she who had called. A man whose voice I don't recognize answers. "Are you my mom?" I apologize for having the wrong number and hang up.

This seemed to last for about 2 hours, and then everything seemed to come back to normal.

The risk? Obvious. What if I needed to call 911. How reliable are the routing directories for cell phones? Are there backup systems in place for 911 routing (one can hope)? Who would I reach? Would they be

able to help?

🔥 Freddie Mac profits misstated due to software error

<Jeremy Epstein <jeremy.epstein@webmethods.com>>

Wed, 9 Nov 2005 09:48:56 -0500

"Freddie Mac will reduce its profit for the first half of 2005 by \$220 million because of an error caused by faulty accounting software, the mortgage finance company said yesterday. ... The error stems from a flaw in the accounting program Freddie Mac has used since 2001. In a recent review of the company's accounting system, Freddie Mac employees realized the software was routinely overstating the amount of interest that the housing finance company earned from certain types of mortgage-backed securities that it bought for investment purposes, spokesman Michael Cosgrove said."

<http://www.washingtonpost.com/wp-dyn/content/article/2005/11/08/AR2005110801778.html>

Nothing very surprising there - I assume there are probably bugs in nearly accounting software, just as there is in all other software. What's surprising is that we don't see these sorts of errors more frequently. Or maybe it's just that this one was big enough that it was noticed, while similar errors exist elsewhere and are never noticed. Again, this shouldn't be surprising - when companies did their books by hand, there were doubtless

always errors, no matter how many people reviewed them.

"Lynn E. Turner, a former chief accountant for the Securities and Exchange

Commission, said this error indicates the company did not adequately test

its accounting systems when they were first installed."

This quote, on the other hand, bothered me. Does this guy understand that

testing can only find the presence of errors, never their absence? Yes, all

of us would like to see more testing, but it's impossible to ever test

enough.

As auditors pay more attention to finances and controls as part of Sarbanes

Oxley reviews, will these sorts of disclosures become more common?

--Jeremy

✦ Some Fast Lane accounts double-billed

<Monty Solomon <monty@roscom.com>>

Fri, 4 Nov 2005 08:45:51 -0500

By Mac Daniel, Globe Staff | November 4, 2005

Fast Lane double-billed 8,498 accounts this week, an error Massachusetts

Turnpike Authority officials attributed yesterday to the electronic toll

company running the system. The computer glitch drew money Tuesday out of

credit card and checking accounts belonging to Fast Lane customers, then

mistakenly docked the same customers Wednesday. The total

wrongly withdrawn
could amount to tens of thousands of dollars, said the Turnpike
spokeswoman,
Mariellen Burns [...]

[http://www.boston.com/news/local/articles/2005/11/04/
some_fast_lane_accounts_double_billed/](http://www.boston.com/news/local/articles/2005/11/04/some_fast_lane_accounts_double_billed/)

✦ Sony CD DRM Blow-Up Continues -- Recalls Ordered, Lawsuits Possible

<Lauren Weinstein <lauren@vortex.com>>
Wed, 16 Nov 2005 13:29:16 -0800 (PST)

The global music giant Sony BMG yesterday announced plans to recall millions of CDs by at least 20 artists -- from the crooners Celine Dion and Neil Diamond to the country-rock act Van Zant -- because they contain copy restriction software that poses risks to the computers of consumers.
[...]

<http://www.nytimes.com/2005/11/16/technology/16sony.html>

Note that in addition to the other problems, the copy protection software in question also apparently tried to establish surreptitious Internet connections with Sony-related servers!

What's really remarkable about this is that any competent outside analysis in advance of the deployment would have raised a dozen different red flags.

I am in general quite sympathetic to concerns about music and film piracy,

but this kind of "shoot self in foot" action by Sony does nothing but hurt the industries' own best interests.

The record labels' and studios' managements need to invite in some *straight talkers* regarding these technical issues -- for high-level consultations, ASAP. -- Lauren

Lauren Weinstein +1 (818) 225-2800 <http://www.pfir.org/lauren>
lauren@pfir.org
PRIVACY Forum - <http://www.vortex.com> <http://lauren.vortex.com>
lauren@eepi.org

[For a nice analysis of the Sony mess, see Bruce Schneier's blog entry:

http://www.schneier.com/blog/archives/2005/11/sonys_drm_rootk.html

The situation is too complicated and in flux for me to summarize here.

PGN]

✈ GPS tracking with Google Maps

<Monty Solomon <monty@roscom.com>>

Mon, 31 Oct 2005 17:02:29 -0500

Developers have created a new pastime, fauxjacking, that mashes together GPS mobile phones and Google Maps. One fauxjacking service, Mologogo, requires only a \$60 GPS-enabled phone and the use of a mobile carrier's Internet services to work. People can use the free, downloadable Mologogo Java application (available at www.mologogo.com) to create real-time visual

records of their movements. Push pins on the Google maps show the times the

tracked device was in a particular location. (Excerpt)

http://www.boston.com/business/personaltech/articles/2005/10/31/new_phones_for_skypers/

'Splogs' Roil Web, and Some Blame Google

<Monty Solomon <monty@roscom.com>>

Wed, 26 Oct 2005 01:24:56 -0400

David Kesmodel, **The Wall Street Journal** online, 19 Oct 2005, B1

Spam, long the scourge of email users, rapidly has become the bane of bloggers too.

Spammers have created millions of Web logs to promote everything from gambling Web sites to pornography. The spam blogs -- known as "splogs" -- often contain gibberish, and are full of links to other Web sites spammers are trying to promote. Because search engines like those of Google Inc., Microsoft Corp. and Yahoo Inc. base their rankings of Web sites, in part, on how many other Web sites link to them, the splogs can help artificially inflate a site's popularity. Some of the phony blogs also carry advertisements, which generate a few cents for the splog's owner each time they are clicked on.

The phony blogs are a particular problem for Google, Microsoft and Yahoo because each offers not only a Web search engine focused on providing the

most relevant results for users but also a service to let bloggers create blogs.

Just this past weekend, Google's popular blog-creation tool, Blogger, was targeted in an apparently coordinated effort to create more than 13,000 splogs, the search giant said. The splogs were laced with popular keywords so that they would appear prominently in blog searches, and several bloggers complained online that that the splogs were gumming up searches for legitimate sites. ...

http://online.wsj.com/public/article/SB112968552226872712-8b51_fijhNltE4s7DX6tvLI9XNo_20061025.html

Whither Goes Google?

<Lauren Weinstein <lauren@vortex.com>>

Sun, 13 Nov 2005 12:13:57 -0800

Google currently represents virtually a textbook example of the complex interplay between innovative, socially positive inventions and developments on one hand, and oppressively dangerous technological arrogance on the other. Or as the fictional David St. Hubbins of the film "This is Spinal Tap" put it more simply around twenty years ago: "It's such a fine line between stupid and clever."

We can look to history for other examples, though the analogies will of

course never be perfect. Microsoft is one recent case where an attitude that many considered to be arrogant appears to have been somewhat tempered by financial, legal, and political realities. Microsoft will survive.

Not so AT&T's "Mother Knows Best" Ma Bell. While the name AT&T will live on as the new moniker of another generally arrogant firm -- SBC Communications -- AT&T for most practical purposes has imploded.

History teaches us much. The controversies over Google Print for Libraries share some aspects with ill-fated attempts to essentially abolish copyrights after the French Revolution -- for the presumed betterment of society.

Attributes such as technological brilliance and visionary thinking can be used not only to describe many at Google, but also the phalanx of individuals who created the atomic bomb for the Manhattan Project. Like those at Google, the minds behind the first nuclear weapons were convinced that they were working for the good of mankind, and -- I believe it's fair to say -- were in many cases blinded by sheer technological enthusiasm to the more ominous aspects of their creations. While Google isn't building physical weapons of mass destruction, a very real mix of extremely potent positive and negative impacts on society, and a range of complex risks that need to be fully understood, are increasingly coming into focus relating to Google's operations.

Such powerful forces can sometimes be managed successfully to truly exclude

evil, but only when those in charge recognize that their own intellects and even good will are insufficient to prevent the "great machines" from being used in ways that can seriously damage individuals and society. It's all too easy not only to be blinded by science, but also to create mechanisms that can be horrendously abused by entities who don't necessarily share the benevolent philosophies of their creators.

There are things that Google could do immediately to potentially ameliorate this situation, but only if their powers-that-be recognize that there are intelligent folks outside of the current Google circle who understand these issues in ways that could avoid a lot of problems for Google -- and for the rest of us.

One relatively simple step would be for Google to create a permanent advisory panel or committee of respected outside individuals well versed on policy and risk issues associated with technology and its impacts on and interactions with society. Such a committee would likely make both public and private reports (the latter protecting proprietary information and plans as appropriate). If such a committee had appropriate access within Google, and if Google were genuinely willing to pay serious attention to the ongoing recommendations of such a group, it is likely not only that future risks to society, but also future risks to Google's own business, could be greatly reduced, and Google's own prospects enhanced as a result.

I can squeeze in one more movie reference. In the classic

science fiction
film "Forbidden Planet" (1956), we learn of a world where a
magnificent and
supremely benevolent race of advanced beings built a gigantic,
fantastic
machine to provide for the physical, intellectual, and spiritual
advancement
of their society. But the Krell, these marvelous creatures,
were so
enmeshed in the project, and so close to the problems that they
were trying
to solve, that they failed to fully understand the implications
of their
creation's power. When they activated their great machine, its
interactions
with the long-suppressed dark side of their minds resulted in
their entire
civilization being destroyed in a single night -- by their own
"creatures
from the Id" -- empowered by the machine itself despite its
noble purpose.

Good intentions don't always equal good results, and forewarned
is
forearmed. Let's do better than the Krell.

Lauren Weinstein Tel: +1 (818) 225-2800 DayThink: [http://
daythink.vortex.com](http://daythink.vortex.com)

Co-Founder, PFIR - People For Internet Responsibility - [http://
www.pfir.org](http://www.pfir.org)

Amex Blue Chip magic!

<"Lindsay Marshall" <Lindsay.Marshall@newcastle.ac.uk>>
Sat, 29 Oct 2005 10:13:11 +0100

http://www.thisisbroken.com/b/2005/10/blue_card_chip.html

[A strange saga on what exactly the Amex Blue Card Chip does,
or how to
get blue chipping away at attempts to get an explanation. PGN]

UK Police Vehicle Movement Database

<"Alan Fitch" <alan.fitch@doulos.com>>

Thu, 17 Nov 2005 09:40:44 -0000

First have a look at this story...

[http://www.theregister.co.uk/2005/11/15/
vehicle_movement_database/](http://www.theregister.co.uk/2005/11/15/vehicle_movement_database/)

Summary: a network of number-plate recognition cameras is being constructed.

These will allow police to find people driving without correct tax and insurance. Conveniently this can be done without a new law.

Now read on... (from a colleague of mine)

> Last night on the way home my number plate was scanned on the M27 and
> reported to the police because the automated records indicated that I had
> not paid my road tax. I was duly stopped by a nice motor cycle police man
> (called Chipps I think... remember the series!) who checked the road tax
> (all duly paid almost a month ago). He then had to spend 5 mins filling
> in a form as this had to be regarded as an official "stop" event, whilst
> muttering that the DVLA only update the system once a month and had the
> most inaccurate updated data in the system!!!.
>

> Hence technology + Automation + DVLA = 5 mins wasted police
time
>
> Now how many motorists re tax each month? and what percentage
> are stopped? So how much waster Police time is that?

For non UK readers

M27 = motorway (UK) / autoroute (France) / autobahn (Germany)
DVLA = Driver Vehicle and Licensing Agency who administer
vehicle taxing
and licensing in the UK

Alan Fitch, Doulos Ltd. Church Hatch, 22 Market Place, Ringwood,
Hampshire,
BH24 1AW, UK +44 (0)1425 471223 <http://www.doulos.com> alan.
fitch@doulos.com

⚡ My approach to CLID / 'phone number privacy issues

<Paul Wexelblat <wex@cs.uml.edu>>

Thu, 27 Oct 2005 13:46:08 -0400

I have my phone listed under a bogus name - The phone company
lets
you use whatever name you want --

1. Cheaper than unlisted - no additional charge
2. Bogus name comes up on CLID - all my friends/acquaintances
know who it is.
3. Marketeers who call (and /only/ marketeers) use the bogus
name -
instant hang-up/ "you have the wrong number"
4. The phone company - if they call - has always used my real
name
(in case you're wondering)
5. It also helps detect direct mail marketeers (who use phone
records
for mailing lists)

6. (No need to block ID)

I have not seen any down side with this approach

(Reverse lookups document the bogus name)

RISKSharvesting@bogusaddress.com

P.M. Wexelblat PhD, Dept. of Computer Science, University of
Massachusetts
Lowell, One University Ave, Lowell, MA 01854

⚡ Re: Cingular: "No password needed" ... (Fenwick, [RISKS-24.08](#))

<Kevin Kadow <kkadow@gmail.com>>

Thu, 10 Nov 2005 19:34:58 -0600

Interestingly, no password was the default for T-Mobile customers for the past several years, but in October the system was updated, and now requires that customers set a password, and T-Mobile now recommends enabling password security, but does provide information on their web site for customers who want to turn the feature off:

T-Mobile recommends that you turn on your VoiceMail password for added security, but the choice is yours.

The risks are obvious--to everyone except decision-makers at Cingular.

Apparently TMO realized the risks -- after massive press coverage of their celebrity customer's voicemail and contact lists being "hacked".

Two books of possible interest

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

Thu, 17 Nov 2005 9:44:06 PST

Christopher Steel, Ramesh Nagappan, Ray Lai

Core Security Patterns:

Best Practices and Strategies for J2EE, Web Services, and
Identity Management

Prentice Hall 2006 (first printing Sep 2005)

Clifford J. Berg

High-Assurance Design:

Architecting Secure and Reliable Enterprise Applications

Addison-Wesley 2006 (first printing Oct 2005)



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 10

Weds 23 November 2005

Contents

- [Voting glitches from the 7 Nov 2005 Election](#)
[Joseph Lorenzo Hall](#)
- [Mode error leads to recall of medical device](#)
[Richard I Cook](#)
- [When switching to backup systems is too costly](#)
[Alan Powell](#)
- [In-car GPS navigation - when it causes an accident](#)
[Mike Scott](#)
- [Bank Shares Suspended After Annual Results Released Early](#)
[David Shaw](#)
- [They needed a real firewall!](#)
[Jeremy Epstein](#)
- [UNH alumni directory misreports 500 deaths](#)
[via Monty Solomon](#)
- ["Chip and PIN" - whose goods are you paying for?](#)
[Andrew Law](#)
- [More Excel risks](#)
[Patrick O'Beirne](#)

- [Irony in certificate-land](#)
[Jeremy Epstein](#)
 - [Risks of applying to law school](#)
[Tony Lima](#)
 - [Producing Error-Free Software is Hard](#)
[J H Haynes](#)
 - [US Military removes Word documents from the Web?](#)
[Diomidis Spinellis](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Voting glitches from the 7 Nov 2005 Election

<Joseph Lorenzo Hall <joehall@gmail.com>>
Tue, 15 Nov 2005 14:12:42 -0800

(The full list is here:
<http://josephhall.org/nqb2/index.php/2005/11/11/2005_glitches>)

Here are some quick summaries of a few very interesting voting glitches that we saw last week. (Listed in order of interest to me.)

[San Joaquin County, California - S.J. County has election night deja vu][1]

San Joaquin County workers misplaced a memory cartridge for an optical-scan machine. They rescanned the ballots and but haven't found the cartridge. In this story, an official says that the new Diebold TSx DREs that they want to use will make things work more smoothly... although the official doesn't recognize that misplacing the memory cartridge in a paperless DRE would not be as easily recoverable (although I believe you'd still have the ballot images resident in memory, no?).

[Cumberland County, Pennsylvania - Software error forces recount in close race for district judge][2]

Two candidates in a race were both mistakenly listed as being from same party. Straight-ticket votes counted both candidates and initially resulted in over-votes. After this was corrected for, the race was down to a 2-vote margin (1703 to 1701 votes). Also see: ["Ballots counted again in judge race"][3]

[Harwinton, Connecticut - Voting machine snafu may lead to challenge in Harwinton][4]

One candidate was endorsed in a race by both Republican and Democratic parties and was listed twice in a choose 2 out of 3 race. This candidate, due to being listed twice, got twice as many votes as the other two candidates in the same contest.

[Pasquotank Co., North Carolina - In Elizabeth City, a 14-vote gap has one candidate calling for a recount][5]

Selecting a certain candidate in the only contest on the ballot resulted in a write-in candidate box being selected instead. The margin in this race was 14 votes. Also, 60 blank ballots were cast (recall that there was only one race for this election). Also see: ["Count on recount in E. City mayor's race"][6]

[Lucas Co., Ohio - State plans to investigate voting chaos; Tuesday's

problems are latest for Lucas County][7]

This one is mysterious: "workers accidentally 'set an option [on the five machines] that prevented the results from being transported onto the memory card.'" Also, massive labor shortage resulted in chaos as election was highly understaffed and a system of "rovers" didn't function correctly (where one elections worker would travel to five polling places to get aggregate totals from machines). Also, see: ["Poll workers blast use of 'rovers'"]][8]

[Montgomery County, Ohio - Vote count goes all night][9]

Various problems resulted in having to download votes from 2000 memory cards instead of from one card each from the 548 precincts. However, during this process, 186 memory cards were found to be missing. After looking through bags of precinct materials ("I voted" stickers, signs, etc.) they had found 171 cards. The remaining 15 cards were only found after rousing pollworkers from bed at 3 am so they could return to the polling place to get the cards either left in machines or lying around the polling place.

[Wichita County, Texas - Human errors hamper voting][10]

35 precincts neglect to perform zeroing out process before election. This resulted in the vote data being impossible to download from the DRE (ES&S) with PEB device. ES&S technicians were able to open the machines, remove the removable memory cards and read the data from there.

[Montgomery County, Ohio - 'Human error' creates doubt about

failed vote in
Carlisle][11]

77 "phantom votes" found to have been cast in an election where a bond measure was defeated by a margin of 146 to 79. ("Phantom votes" are when there are more votes counted than there are registered voters that could have cast votes) In this case, there were only 148 registered voters that could have cast votes in this race.

[1]: <http://www.recordnet.com/apps/pbcs.dll/article?AID=/20051110/NEWS01/511100320/1001>

[2]: <http://www.pennlive.com/politics/patriotnews/index.ssf?/base/news/1131618230305160.xml&coll=1>

[3]: <http://www.cumberlink.com/articles/2005/11/12/news/news08.txt>

[4]: <http://www.rep-am.com/story.php?id=30053>

[5]: <http://home.hamptonroads.com/stories/story.cfm?story=95098&ran=37812>

[6]: <http://home.hamptonroads.com/stories/story.cfm?story=95171&ran=188639>

[7]: <http://toledoblade.com/apps/pbcs.dll/article?AID=/20051110/NEWS09/511100477>

[8]: <http://toledoblade.com/apps/pbcs.dll/article?AID=/20051112/NEWS09/511120462>

[9]: <http://www.daytondailynews.com/localnews/content/localnews/daily/1110voting.html>

[10]: http://www.timesrecordnews.com/trn/local_news/article/0,1891,TRN_5784_4226503,00.html

[11]: <http://www.daytondailynews.com/localnews/content/localnews/daily/1112carlislevote.html>

Joseph Lorenzo Hall, PhD Student, UC Berkeley, School of Information (SIMS)

<<http://josephhall.org/>>

⚡ Mode error leads to recall of medical device

<Richard I Cook <ri-cook@uchicago.edu>>

Fri, 28 Oct 2005 07:05:28 -0500

The U.S. Food and Drug Administration Medwatch program has issued a warning based on the possibility of mode error that can lead diabetics to misread their home glucose monitor. The FDA's Medwatch program, which issued the warning, receives user and facility reports of problems with medical devices. The device provides glucose values in either American or European standard units (mg/dl or mmol/liter) based on setting in the device. That setting may be changed when users are trying to set the date or time fields in the device. The FDA News also notes reports that the setting may change when the meter is dropped or its battery is changed.

The devices involved, a set of Abbott blood glucose monitors used by diabetics for home glucose monitoring, have not been recalled by the manufacturer. Abbott issued a press release on October 14, 2005 acknowledging the fault and is undertaking "a worldwide correction and notification to all healthcare professionals and users, when known, about the measurement switching problem" according to the FDA announcement.

Abbott manufactures the devices for resale under a variety of brand names. The U.S. brand names involved include FreeStyle, FreeStyle Flash, FreeStyle Tracker, Precision Xtra, MediSense, Sof-Tact,

Precision Sof-Tact, MediSense, Optium, and private label brands ReliOn Ultima, Rite Aid, and Kroger blood glucose meters. Precision Sof-Tact meters, which were inadvertently omitted from Abbott's press release, are also included. Outside the U.S. the involved brand names are Xceed, Liberty, Boots, Xtra Classic, Easy, and SofTrac. These products are distributed primarily through retail and mail order pharmacies and physicians' offices.

Problems with blood glucose meters are not uncommon. Earlier this year Lifescan Inc, a subsidiary of Johnson & Johnson, issued a Class I Recall notice for its OneTouch SureStep blood glucose meter because of reports of failure of some segments of its LCD display that could lead users to believe that their glucose was normal when it was actually dangerously high. Class I recalls are "for dangerous or defective products that predictably could cause serious health problems or death. Examples of products that could fall into this category are a food found to contain botulinal toxin, food with undeclared allergens, a label mix-up on a life saving drug, or a defective artificial heart valve."

Mode errors are among the more common forms of human-computer interaction problems. A classic paper on mode errors in the cockpit is "How in the world did I ever get into that mode?: Mode error and awareness in supervisory control" (Sarter, ND and D Woods, Human Factors 37, 5-19). Mode errors are a common problems with medical devices, especially relating to units of

measurement. An example is shown at http://www.ctlab.org/Mode_Error.cfm Such problems are usually treated by manufacturers as a type of operator error and are usually incredulous regarding the contribution of device design to mode error. Glucose meters are ubiquitous because glucose control is the centerpiece of diabetes management. .

- - - - -

Links of interest:

Short description of "mode error" with example:

http://www.ctlab.org/Mode_Error.cfm

Links regarding the Abbott products:

FDA Medwatch:

<http://www.fda.gov/medwatch/safety/2005/safety05.htm#glucose>

FDA News (announcement):

<http://www.fda.gov/bbs/topics/NEWS/2005/NEW01250.html>

Abbott Laboratories website:

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

Abbott Laboratories "urgent correction" notice:

http://www.abbott.com/news/press_release.cfm?id=1006

Abbott units of measure table:

http://www.abbottdiabetescare.com/news/measurement_units.aspx

Links regarding the Lifescan products:

FDA Medwatch:

<http://www.fda.gov/medwatch/safety/2005/safety05.htm#LifeScan>

FDA Firm Safety Alert:

http://www.fda.gov/oc/po/firmrecalls/lifescan04_05.html

FDA Class I Recall noticee:

<http://www.fda.gov/cdrh/recalls/recall-041105.html>

Johnson & Johnson's Lifescan urgent recall notice (with example):

http://www.lifescan.com/company/about/press/surestep_display/

FDA Recall classifications:

<http://www.cfsan.fda.gov/~lrd/recall2.html>

Richard Cook, MD, Cognitive Technologies Laboratory, University of Chicago

(I have no commercial relationship with any pharmaceutical company or device manufacturer)

Richard I. Cook, MD, Assoc.Prof., Department of Anesthesia and Critical Care
Director, Cognitive Technologies Laboratory Univ. of Chicago 1-773-702-4890

⚡ When switching to backup systems is too costly

<Alan Powell <rfc826@yahoo.com>>

Mon, 31 Oct 2005 05:18:45 +0000 (GMT)

On Friday 28 Oct '05, Standard Bank's (<http://www.standardbank.co.za>) ATM

network started declining 30% of transactions [i.e., you couldn't withdraw money].

A Standard Bank spokesman claimed:

* The problem was due to a "lack of capacity at the central processing unit".

* A "management decision" had been taken to not switch to the backup system until non-peak hours because the switch-over would take 40 minutes during which time the entire ATM network [country-wide!] would be offline.

* The fault arose additional processing capacity had been added to the centra processing unit to cater for the busy season.

[Anyone care to enumerate all the ways they could improve on the availability and redundancy of their system?]

✶ In-car GPS navigation - when it causes an accident

<Mike Scott <usenet.9@scotts.dnsalias.com>>

Thu, 27 Oct 2005 12:07:34 +0100

I've been wondering about getting an in-car GPS navigator, but I'm beginning to wonder about the wisdom of this.

My son was being driven by a friend in London. The friend's car was equipped with some sort of GPS navigation. They were driving eastbound along the north side of the River Thames, intending to cross at Tower bridge to a destination on the south side of the river. The GPS said "turn right" when they reached the bridge. The only snag is that this is a one-way system. To cross the bridge you turn left, *away* from the bridge, and drive right round the block. Unfortunately, said friend payed more attention to the GPS than the road signing, and very nearly collided with a car coming the other way.

I now wonder what liability the makers of such equipment have. At the very least, an inaccurate system can be a distraction on a busy road, and conflicts in data to a driver can cause delays in reaction. At worst, it could cause a fatal accident.

Incidentally, I get very irked by my Garmin GPS72, which powers up with a screen that says "All data is presented for reference only. You [the user] assume total responsibility and risk...." Yet from their website: "Garmin products make it easy to get there and back. These rugged navigators are built to handle the Great Outdoors -- and still keep you on track." I'm not sure they can have it both ways!

🚨 Bank Shares Suspended After Annual Results Released Early

<David Shaw <dshaw@avaya.com>>

Thu, 3 Nov 2005 09:49:40 +1100

Westpac (www.westpac.com.au), a large Australian bank, was forced to halt trading on its shares and deliver its annual profit briefing a day early after it accidentally sent its results by email to research analysts.

A template containing past results was sent to analysts. It was soon discovered that the new figures were embedded in the spreadsheet and were accessible with via "a minor manipulation". Analysts telephoned the bank to report the error and the template was recalled.

But the damage was done. The Australian Stock Exchange was notified and trading was suspended as it appeared that some people had access to information not generally available to the market. The bank then brought

forward its results announcement.

Westpac Chief Financial Officer, Philip Chronican, said there was no evidence that the figures had been circulated and there were no signs of disorderly trading in Westpac shares. He added: "It is not just one error, it is a compounding of two or three errors ... We will obviously be conducting a full inquiry to make sure it doesn't happen again."

More detail at: <http://www.smh.com.au/news/business/westpac-jumps-the-gun-on-profit/2005/11/02/1130823280336.html>

⚡ They needed a real firewall!

<Jeremy Epstein <jeremy.epstein@webmethods.com>>

Thu, 3 Nov 2005 09:04:07 -0800

I received this note today:

> Due to a serious fire at the University of Southampton, UK, the
> www2006.org website and mailing lists are temporarily
unavailable. [...]

>

> Information about the fire can be found at:

> <http://news.bbc.co.uk/1/hi/england/hampshire/4390048.stm>

Perhaps they needed a real (physical/architectural) firewall to protect their servers?

More seriously, just a reminder that as much as we worry about cybersecurity, physical problems can be just as serious a threat to continuity. [The report indicates that the fire was accidental; whether the

destruction was accidental or intentional, it's a very effective
Denial of
Service.]

✶ UNH alumni directory misreports 500 deaths

<Monty Solomon <monty@roscom.com>>

Fri, 4 Nov 2005 08:47:36 -0500

On 2 Nov 2005, 63-year-old Sandra Keans was preparing for her City Council race. The next day, she discovered that she and 500 other graduates of the University of New Hampshire had been listed as deceased in the annual alumni directory. This was attributed to "a foible of fatal proportions" resulting from a publishing technician's error. [Source: 'Dead' alumni walking: UNH report of their demise greatly exaggerated Maria Cramer and Emma Stickgold,

The Boston Globe, 4 Nov 2005; PGN-ed]

http://www.boston.com/news/local/articles/2005/11/04/dead_alumni_walking/

✶ "Chip and PIN" - whose goods are you paying for?

<"Andrew Law" <alaw@hgl-dynamics.com>>

Tue, 15 Nov 2005 12:47:31 -0000

Over the last few months, almost all UK retailers who can take credit or debit card payments have been switching to the use of "Chip and PIN" card

readers instead of the older system in which the customer signs a sales invoice. The card reader scans the customer card, the customer then types in his or her PIN to the numeric keypad on the reader, and the system then verifies that the card details and PIN match. This is believed to be more secure than relying on signatures, which in general is probably true. However, it may lead to some interesting side effects...

Last week, one of my colleagues was in the Waitrose supermarket near our office. When she came to pay with her credit card, she was asked to type per PIN into the keypad as normal. As the cashier was handing the receipts over, she spotted something rather odd. The itemised till receipt correctly showed the goods which she had taken from the shelves and which had been scanned in by the barcode reader at the checkout. The sales receipt, however, showed a different amount, indicating that she had been billed for the wrong amount. My colleague and the cashier realised that she had in fact paid an amount which exactly matched the value of the goods of the previous customer, who had paid by cash instead of credit card.

After having spotted that there was a discrepancy, it took 20 minutes for a supervisor to sort out the mess.

The RISK here would seem to be that the "chip and PIN" system is not automatically synchronised with the rest of the checkout, and that customers may be being charged for the wrong amount on an ongoing basis if the cashier is not aware to check the receipts for consistency.

This morning, our local supermarket has reverted to using the signature method for checking identity.

Andy Law
alaw@hgl-dynamics.com

⚡ More Excel risks

<"Patrick O'Beirne" <yg05@sysmod.com>>
Fri, 04 Nov 2005 10:02:49 +0000

Seen on the Excel-L list:
(Blacked out squares indeed - somebody thought that black shading would hide text!)
- - - -
<Start of copied data>

Westpac was forced to halt trading on its shares and deliver its annual profit briefing a day early after it accidentally sent its results by email to research analysts.

Details of the \$2.818 billion record profit result for the 12 months to September 30, which were due to be announced this morning, were overshadowed by concerns that some information may have been leaked to the market.

The new figures were embedded in a template of last year's results and were accessible with minor manipulation of the spreadsheet.

"A trading halt is not a trivial issue and therefore not a decision we took

lightly," Mr Chronican said.

"It is not just one error, it is a compounding of two or three errors.

We will obviously be conducting a full inquiry to make sure it doesn't

happen again."

<end of copied data>

Source:

<http://www.zdnet.com.au/news/security/soa/>

[E_mail_bungle_leaves_Westpac_red_faced/0,2000061744,39220583,00.htm?feed=rss](http://www.zdnet.com.au/news/security/soa/E_mail_bungle_leaves_Westpac_red_faced/0,2000061744,39220583,00.htm?feed=rss)

<http://www.smh.com.au/news/business/westpac-jumps-the-gun-on-profit/2005/11/02/1130823280336.html>

- - - -

Another one for the collection, from Richard on the Excel-L list:
File Properties can be changed even in 'protected' workbook

>Just another oh-by-the-way...

>

>use the workbook properties with caution. I used to store various version

>info here, but later realised that this can be accessed and changed by

>using windows explorer.

>

>Even if the structure of the workbook is password protected (preventing a

>normal user from accessing the workbook properties tabs)

>

>Nifty eh?

>

>Richard

>

> - - - -

>The EXCEL-L list is hosted on a Windows NT(TM) machine running L-Soft

>international's LISTSERV(R) software. For subscription/signoff

info

>and archives, see <http://peach.ease.lsoft.com/archives/excel-1.html> .

Patrick O'Beirne FICS, Systems Modelling Ltd. +353 55 22294
<http://www.sysmod.com/> Spreadsheet Auditing Methodology <http://sysmod.buy.ie>

Irony in certificate-land

<Jeremy Epstein <jeremy.epstein@webmethods.com>>

Thu, 27 Oct 2005 15:01:21 -0400

It always amuses me when security companies mess up their security. If you're planning to attend the RSA Conference, you can go to <http://2006.rsaconference.com/us/register/travel.aspx>, which points you to their travel agency at https://www.meetingpartners.com/RSA_Conf_2006/. The latter has an expired certificate.

You'd think that RSA, of all folks, would ensure that their certificates are valid....

Risks of applying to law school

<Tony Lima <tonylima2@att.net>>

Thu, 10 Nov 2005 10:44:21 -0800

No, not the risks you're thinking of.

A friend is applying to law school. He's young but knows something about computers. Law schools collaborate with the Law School Admissions Council (<http://www.lsac.org>) to use a single application form. This form is created using OmniForm (published by Nuance, formerly known as ScanSoft). OmniForm requires that you install an ActiveX control on your computer. This control apparently only works on Windows computers. Macs are not welcome. (So much for "Legally Blonde.") Linux and other flavors of UNIX are beyond the pale.

My friend was mumbling obscenities about installing this control. The computer he was working on apparently died during the process so I took a deep breath and said he could work with my notebook computer. He dug into the application, got to the ActiveX installation screen and the control refused to install. At that point I took over (not wanting him messing with my security settings). I finally got the control to install after doing the following:

- Disabling my anti-spyware software (ewido security suite). I then tried to install the control with no luck.
- Setting the privacy permission for lsac.org to "allow." Again no luck installing the control.
- Eliminating all security by making the security settings (Tools/Internet Options/Security/Custom Level) completely open. I enabled each and every ActiveX and other control including unsigned controls and

controls marked as
not safe. The control then installed successfully.

Now perhaps I didn't have to go quite that far but a deadline was approaching and I really didn't want to take the time to perform the trial and error that would apparently be required to determine exactly how much security to give up.

It occurs to me that this is truly THE law school admission test. If you're dumb enough to let this control install you're probably good law school material. OTOH if you don't let the control through then you're too smart to be a lawyer. (That's about all the humor I can manage after 1.5 hours fighting with this stuff. I've disconnected from the net and am running my usual four scanning programs right now.)

Tony Lima, Prof. of Economics, California State University, East Bay
tony.lima@csueastbay.edu (510) 885-3889

⚡ Producing Error-Free Software is Hard

<jhhaynes@earthlink.net>
Mon, 14 Nov 2005 20:11:03 -0600 (CST)

I installed a more recent release of Linux on two desktop machines with no problems. When I tried to do a similar upgrade on my laptop I ran into trouble. The X window system produced a blank white screen instead of a functioning window system.

Checking with a discussion board revealed that several other people were having the same problem, and called it several different things. It did seem to involve certain makes of video hardware. I found a pointer to a bug tracking system run by the people who produce the Linux distribution.

The bug had been reported there, several times in fact, and eventually the several bugs were recognized as being the same and were merged into one. Someone had figured out which library module of the X window system was causing them problem. He suggested a work-around of replacing that module with the one from the previous release of Linux, since that would restore correct operation.

Someone figured out exactly which line of code was causing the problem. It was being completely optimized away by the compiler, and needed to be executed repeatedly. He suggested a way to change the code so it would not be optimized away, or compile with less aggressive optimization, or compile with a previous version of the compiler. Changing the code was rejected on the grounds that there might be hundreds of other instances of the same code throughout the system. They would all have to be located and changed to insure correct operation.

So the problem escaped being referred to the X window system people and was instead referred to the compiler people. They studied the offending line of code and discussed at some length whether it was or was not correct behavior

for the compiler to optimize it away. Some were of the opinion that the problem should be referred to the keepers of the C language specification, since there was disagreement about what the compiler should do with such a line of code. But one of their number decided that ambiguity or not, updating the compiler should not break things that previously worked unless the previous behavior was demonstrably wrong; so he made a change to the compiler.

This was picked up by the keepers of the Linux distribution, who made the updated compiler available and then recompiled the X window system and made that available as an update. One could argue whether they should have recompiled the entire distribution, since there is no telling how many other programs and libraries in the system might be affected by the compiler anomaly. Not doing so seems reasonable enough, since it would take resources away from fixing other bugs that have other causes.

✦ US Military removes Word documents from the Web?

<Diomidis Spinellis <dds@aueb.gr>>

Wed, 09 Nov 2005 19:25:34 +0300

In [RISKS-23.50](#) ("U.S. military sites offer a quarter million Microsoft Word documents"), I wrote about the large number of Microsoft Word documents visible on US military sites (sites in the .mil domain) through

Google

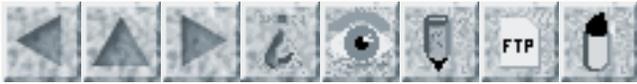
searches. The article documented how such documents could lead to the leakage of confidential data. A week later I set up a script to watch the number of Word documents available through Google searches on various TLDs to see if and when the military would recognize the threat those documents posed and remove them.

According to the data I gathered the number of Word documents in .mil sites returned by Google peaked at 1,180,000 on September 20th 2005, and then started gradually declining. Currently there are 942,000 documents online. No such decline was visible on other domains I monitored, so the change is probably not an artifact of Google's collection or query mechanisms, but an organized move by the US military. Maybe somebody understood the risk associated with these documents and was in a position to act.

I've placed the charts illustrating the trends online at <http://www.spinellis.gr/blog/20051109/>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 11

Weds 7 December 2005

Contents

- [Hospital operates on wrong patient](#)
[Walter F. Roche Jr.](#)
- [Mercedes brake test fiasco](#)
[Andre Kramer](#)
- [Tens of thousands mistakenly put on terrorist watch lists](#)
[Anne Broache via Richard M. Smith](#)
- [Security Flaw Allows Wiretaps to Be Evaded, Study Finds](#)
[John Schwartz and John Markoff via David Farber](#)
- [DHS-Sponsored phishing report](#)
[Aaron Emigh](#)
- [Poorly designed online interfaces make identity theft simple](#)
[Marty Lyons](#)
- [School psychologist's student records accidentally posted online](#)
[Monty Solomon](#)
- [Plain-text passwords: as RISKy as you'd think](#)
[Steve Summit](#)
- [Y2K++](#)
[Jim Horning](#)

- [Risks of naive date calculation](#)
[Mike Albaugh](#)
 - [Bye Bye BlackBerry?](#)
[Ian Austen via Monty Solomon](#)
 - [SafetyText](#)
[Nick Brown](#)
 - [Data disasters dog computer users](#)
[Amos Shapir](#)
 - [Online tax credit system closed](#)
[Amos Shapir](#)
 - [Re: Some Fast Lane accounts double-billed](#)
[Steve Summit](#)
 - [Stop speeding using a GPS?](#)
[Jeremy Epstein](#)
 - [Re: In-car GPS navigation](#)
[Henry Baker](#) [Derek P Schatz](#) [Ian Chard](#) [Jack Christensen](#)
 - [Re: UK Police Vehicle Movement Database](#)
[Identity withheld](#) [mathew](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Hospital operates on wrong patient

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

Fri, 2 Dec 2005 9:16:32 PST

In 1999, a 47-year-old woman was diagnosed with breast cancer in Magee-Womens Hospital (part of the U. Pittsburgh Medical Center), and underwent a mastectomy. It was later discovered that the hospital lab had switched biopsy specimens. Ten cases against the hospital are now pending in state courts, even though the hospital has passed federal inspections. Similar lawsuits and complaints name other medical centers.

* In Maryland, a hospital lab sent out hundreds of HIV and hepatitis test results despite data showing that the results might be invalid and mistakenly lead infected patients to believe they were disease-free. The same laboratory had just received a top rating from CAP inspectors.

* In Yakima, Wash., eight emergency room doctors walked off their jobs to protest hospital deficiencies they said included lab mistakes, such as mixed-up blood samples. CAP had declared the lab "in good standing" the year before.

* At the famed Mayo Clinic in Minnesota, an allegedly misdiagnosed gall bladder cancer case led to revelations of a close relationship between the clinic and CAP. A Mayo pathologist serving on a CAP advisory panel twice sought and obtained accreditation renewals despite unacceptable lab practices cited by CAP inspectors.

[Source: Walter F. Roche Jr., Lab Mistakes Threaten Credibility, Spur Lawsuits: Some top medical facilities are scrutinized as errors mount and oversight is questioned, *Los Angeles Times*, 2 Dec 2005; PGN-ed] <http://www.latimes.com/news/nationworld/nation/la-na-labs2dec02,0,3901421.story?coll=la-home-headlines>

[Thanks to Lauren Weinstein for contributing this article. PGN]

Mercedes brake test fiasco

<"Andre Kramer" <andre.kramer@eu.citrix.com>>

Thu, 1 Dec 2005 09:59:25 -0000

The Register reports that an automotive journalist was fired for rigging a radar enhanced (assumedly computer controlled) automobile brake system demonstration. Apparently, the Mercedes engineers (under duress) helped simulate the demonstration, which could not have worked in an enclosed space, by manual braking. However, the demo went badly wrong and the article

http://www.theregister.co.uk/2005/11/29/mercedes_brake_test_fiasco/

correctly identified the risk of false trust in a new system that would have resulted from the attempted smoke and black mirrors going undetected. [Risks of lack of feedback from expensive car suspension systems could also be noted.]

✶ Tens of thousands mistakenly put on terrorist watch lists

<"Richard M. Smith" <rms@computerbytesman.com>>

December 6, 2005 10:11:36 PM EST

http://www.nytimes.com/cnet/CNET_2100-7348_3-5984673.html?pagewanted=print

Tens of thousands mistakenly put on terrorist watch lists
Anne Broache, Staff Writer, CNET News.com
December 6, 2005

Nearly 30,000 airline passengers discovered in the past year that they were mistakenly placed on federal "terrorist" watch

lists, a
transportation security official said Tuesday.

Jim Kennedy, director of the Transportation Security Administration's redress office, revealed the errors at a quarterly meeting convened here by the U.S. Department of Homeland Security's Data Privacy and Integrity Advisory Committee.

Marcia Hofmann, staff counsel at the Electronic Privacy Information Center, said this appeared to be the first time such a large error has been admitted. "It was a novel figure to me," Hofmann said. "The figure shows that many more passengers than we've anticipated have encountered difficulty at airports. The watch list still has a long way to go before it does what it's supposed to do."

Kennedy said that travelers have had to ask the TSA to remove their names from watch lists by submitting a "Passenger Identity Verification Form" and three notarized identification documents. On average, he said, it takes officials 45 to 60 days to evaluate the request and make any necessary changes.

Travelers have been instructed to file the forms only after experiencing "repeated" travel delays, he said, because additional screening can occur for multiple reasons, including fitting a certain profile, flying on a one-way ticket, or being selected randomly by a computer. ...

EPIC_IDOF@mailman.epic.org

https://mailman.epic.org/cgi-bin/mailman/listinfo/epic_idof

Security Flaw Allows Wiretaps to Be Evaded, Study Finds [from IP]

<David Farber <dave@farber.net>>

Wed, 30 Nov 2005 06:54:22 -0500

The technology used for decades by law enforcement agents to wiretap telephones has a security flaw that allows the person being wiretapped to stop the recorder remotely, according to research by computer security experts who studied the system. It is also possible to falsify the numbers dialed, they said. Someone being wiretapped can easily employ these "devastating countermeasures" with off-the-shelf equipment, said the lead researcher, Matt Blaze, an associate professor of computer and information science at the University of Pennsylvania. "This has implications not only for the accuracy of the intelligence that can be obtained from these taps, but also for the acceptability and weight of legal evidence derived from it," Mr. Blaze and his colleagues wrote in a paper that will be published today in *Security & Privacy*, a journal of the Institute of Electrical and Electronics Engineers. [...]

[Source: John Schwartz and John Markoff, **The New York Times**, 30 Nov 2005]

⚡ DHS-Sponsored phishing report

<"Aaron Emigh" <aaron@radixlabs.com>>

Tue, 29 Nov 2005 01:11:02 -0800

Online identity theft, a.k.a. "phishing," refers to attacks that exploit a wide variety of RISKS, using both technology and social engineering, to illicitly obtain and profit from confidential information. A new report on online identity theft, sponsored by the US Department of Homeland Security and SRI International, provides a holistic treatment of the subject. The report discusses technologies used by phishers, breaks down the flow of information in a phishing attack, identifies chokepoints at which an attack can be thwarted, and discusses technical countermeasures that can be applied at each chokepoint. While technology alone cannot solve the phishing problem, substantial opportunities to mitigate the losses are identified.

The report is titled "Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures," and is available at <http://www.anti-phishing.org/Phishing-dhs-report.pdf>.

Aaron Emigh, Radix Labs, 415-297-1305

⚡ Poorly designed online interfaces make identity theft simple

<Marty Lyons <marty@martylyons.com>>

Thu, 17 Nov 2005 13:11:22 -0800

I recently had to renew my membership with the American Automobile Association (the equivalent to the CAA in Canada, or the RAC in the UK). In the past there was no web interface, but AAA has now moved online. To sign up for an account, I needed to supply a membership number (printed on your plastic member card), and my name (also printed on the card), along with an email address, and a chosen account name. A few seconds later, I was logged in, and was able to check my account info, including mailing address, and type of credit card used for membership.

There was no verification of identity at all during account establishment.

At a minimum, mandating that a user-entered postal code match the AAA database prior to creating the account would have afforded some protection.

So with a AAA member number and name, someone is well on their way to identity theft -- the rest of your wallet not required. Since many places take AAA cards to provide discounted services (hotels, car repair, restaurants, movie theatres, etc.) you can imagine the RISK. I've sent a letter to the organization letting them know their web registration needs to be redesigned.

⚡ School psychologist's student records accidentally posted online

<Monty Solomon <monty@roscom.com>>

Sat, 3 Dec 2005 13:47:29 -0500

A school psychologist's records detailing students' confidential information and personal struggles were accidentally posted to the school system's Web site and were publicly available for at least four months. A reporter for *The Salem News* [Mass.] discovered the records last week and alerted school officials, the newspaper said in a story Friday. To protect students' privacy, the newspaper said it withheld publishing the story until the documents were removed from the Internet, which occurred Wednesday. [...]

[Source: *The Boston Globe*, 2 Dec 2005; PGN-ed]

http://www.boston.com/news/education/k_12/articles/2005/12/02/school_psychologists_student_records_accidentally_posted_online/

✶ Plain-text passwords: as RISKy as you'd think

<Steve Summit <scs@eskimo.com>>

Fri, 18 Nov 2005 12:55:57 -0500

A nice report of an investigation into how many plain-text passwords one can almost trivially sniff in public-access places like hotels, conference centers, and open wireless hotspots:

http://www.infoworld.com/article/05/11/04/450Psecadvise_1.html

The article also makes the point that although the passwords so sniffed are often "unimportant" ones, for services such as mere e-mail access or gambling site logins, people are often known to use their same passwords for

these and for their "secure" systems such as Windows network logins.

I came across this link in Bruce Schneier's excellent "Crypto-Gram" newsletter at <http://www.schneier.com/crypto-gram.html>, which I'm sure is known to many RISKS readers, but which I had neglected to read in a while. It's worth keeping up with.

Y2K++

<"Jim Horning" <Jim.Horning@sparta.com>>

Wed, 30 Nov 2005 11:53:33 -0800

My employer has outsourced the administration of its 401(k) plan to TruSource, a division of Union Bank of California, N.A. This week I received annual enrollment material from TruSource. It contains generic blurbs about 401(k)s and retirement planning, in addition to material particular to our plan. Part of the latter is a summary page for each of the available investment options. These pages are clearly labeled "Copyright (c) Standard & Poor's, a division of The McGraw-Hill Companies."

The page for each fund contains a graph of "GROWTH OF \$10,000." I think the format and content are specified by the SEC, and they are presumably automatically generated from some kind of database. For some reason, I happened to look more closely than usual at one of the charts,

and noticed something odd about the labeling of the year axis, and started inspecting them all. Most of them contain dates in the 31st and 41st centuries!

For example, the chart for the Pioneer High Yield Fund "(SINCE 03/31/98)" is labeled with consecutive years

4098 3099 2000 1001 4001 4002 2003 1004 4004 3005

Apparently the dates escaped the notice of the humans (if any) at McGraw-Hill and TruSource who were in the loop in the preparation of these documents. It is interesting to speculate what combination of programming errors would yield this precise sequence of dates.

Jim H. <http://horning.blogspot.com>

⚡ Risks of naive date calculation

<Mike Albaugh <albaugh@perilin.com>>

Wed, 23 Nov 2005 12:48:48 -0700

I have in my possession a box of Nyakers (that should be an A-ring, BTW)

"Authentic Swedish Apple Snaps" that is

BEST BEFORE 29 FEB 2006

Lazy Programmer? Faulty date-manipulation library? Or do the Swedes know

something about the depths to which lawmakers will stoop in calendar

manipulation?

The computer scientist in me wants to know if the comparison to a (currently) non-existent date should:

- * always fail (Cookies are stale now),
- * always succeed (Cookies will never get stale)
- * throw an exception (Cookies should not exist in this universe)

🔥 Bye Bye BlackBerry?

<Monty Solomon <monty@roscom.com>>

Sun, 4 Dec 2005 01:45:19 -0500

A ``long-running patent infringement battle between the maker of BlackBerry, Research In Motion, and NTP, a tiny patent holding company, might cause a service shutdown, perhaps within a month. ... R.I.M., which is based in Waterloo, Ontario, promises it has a solution that will keep its beloved BlackBerries humming even in the face of an injunction. While most analysts view the prospects of a shutdown as unlikely, they have little faith in the proposed solution, which has potential legal pitfalls of its own. What's more, the history of the struggle between the companies means that no outcome is certain.''

[Source: Ian Austen, Bye Bye BlackBerry?, What if your BlackBerry screen went dark? *The New York Times*, 3 Dec 2005; PGN-ed]

<http://www.nytimes.com/2005/12/03/technology/03blackberry.html?ex=1291266000&en=df205fd24ccb8593&ei=5090>

SafetyText

<Nick Brown <Nick.BROWN@coe.int>>

Mon, 28 Nov 2005 17:17:20 +0100

A new UK-based service called SafetyText (<http://www.safetytext.com/>)

enables you to send a text message which will be delivered after a certain delay unless canceled.

The idea seems to be that, before exposing yourself to danger, you send a text - say, "Help, I'm being attacked by rabid bats" before entering a cave - and then it will be sent if you don't emerge from the cave in time to cancel it.

The risks are left as an exercise to the reader, but here are some pointers to get you started:

- SMS messaging delivery is inherently unreliable, so maybe your "help" text won't get through...
- ... or maybe your "cancel" text won't get through.
- Many people receiving such a text, regardless of how it's phrased, will tend to assume the worst (despite the "don't panic" instructions on the service's Web site) and will send in the emergency services on a possibly unnecessary search for someone who just happens to be out of GSM service range.

I'm also slightly worried that the same short number used for the SafetyText

service - 63344 - appears in the banner advert above the site's start page, which at the present time invites me to send the name of Coldplay's lead singer to win tickets to see them in concert. I hope they don't launch a particularly popular game while I'm being attacked by the rabid bats.

⚡ Data disasters dog computer users

<"Amos Shapir" <amos083@hotmail.com>>
Wed, 07 Dec 2005 14:58:20 +0200

A laptop crammed with dead cockroaches tops a list of data disasters compiled by computer experts.

<http://news.bbc.co.uk/go/em/-/2/hi/technology/4500482.stm>

[That would be a tough roach to hoe. PGN]

⚡ Online tax credit system closed

<"Amos Shapir" <amos083@hotmail.com>>
Mon, 05 Dec 2005 17:12:37 +0200

Organised fraud forces HM Revenue and Customs to stop accepting online applications for tax credits. Full story:

<http://news.bbc.co.uk/go/em/-/2/hi/business/4493008.stm>

Re: Some Fast Lane accounts double-billed (Solomon, [RISKS 24.09](#))

<Steve Summit <scs@eskimo.com>>

Sun, 04 Dec 2005 14:17:37 -0500

Monty Solomon forwarded an item to [RISKS 24.09](#) about a batch of Massachusetts Turnpike drivers who were doubly charged for their electronic tolls, due to one day's worth of records being mistakenly processed twice.

If anyone's keeping a canonical list of "bugs that are way easy to make and deserve special handling", this scenario clearly belongs.

We've been hearing variations on the same song for decades: it used to be the phone company accidentally double-running a billing tape containing the call records from a long-distance switch, but to this day it can still easily happen any time there are batches of transactions created by system A and later processed or reconciled on separate system or subsystem B. (And I can't personally be at all smug about this: in a former life I ran a small, simple, homebrew, but high-volume e-commerce site, and I committed this same mistake once or twice myself. Fortunately I was also in a position to synthesize and inject automatic refunds to the credit card accounts of affected customers, well before most of them even noticed.)

I'm sure that any organization large enough to address this risk responsibly has implemented the obvious sorts of double-checks (perhaps

involving explicit batch serial numbers which are logged and checked

by the processing system, in order to reject inadvertent duplicates).

But since the need for such double-checks is all too likely to be recognized only *after* the double-billing problem has bitten a particular system at least once, and since new systems having this

vulnerability are continually being written, it's a problem that, unfortunately, will continue to happen.

✶ Stop speeding using a GPS?

<Jeremy Epstein <jeremy.epstein@cox.net>>

Sun, 4 Dec 2005 15:06:26 -0500

Transport Canada is testing a device that figures out where you are using

GPS, and causes your car to increase the resistance in the gas pedal if you

try to exceed the speed limit.

Bad idea. I'm not an expert in GPS systems, but I've seen them get

confused, especially when there are nearby parallel roads. I wouldn't want

it to hold my speed to 25 MPH because it thinks I'm on the dirt road that

runs parallel to a highway. And if the device changes its mind suddenly,

the results could be catastrophic - I'm pushing hard on the accelerator

because (for whatever reason) I decide to exceed the speed limit, and

suddenly it decides the speed limit has increased - now I'm flooring the car

because it reduces its resistance factor. Conversely, if I have a normal

pressure on the accelerator, and the speed limit drops, the

device might

cause my speed to drop precipitously. I'm sure there are lots of other GPS-based risks - what does the device do if it can't find a GPS signal?

Hopefully the designers of the device considered the risks, but the article doesn't mention any - only the advantages of improved road safety, reduced fuel usage, etc.

Article at http://www.cnn.com/2005/AUTOS/12/01/canada_gps_speed/index.html

which references a Toronto Globe & Mail article at <http://www.globetechnology.com/servlet/story/RTGAM.20051128.gtsmartcars28/BNPrint/Technology/>

Re: In-car GPS navigation (Scott, [RISKS-24.10](#))

<Henry Baker <hbaker1@pipeline.com>>

Sun, 27 Nov 2005 18:09:42 -0800

For the last year or so, if you rented a Hertz car with its "Neverlost" (Magellan) GPS system, you couldn't get out of Boston's Logan Airport -- at least if you listened to the "Neverlost" system. It tried to route you onto a one-way street in the airport itself (the other direction was closed off due to construction). Now everyone who has been in Boston in the last several years knows about the construction at the airport and the Big Dig, but here's a system that clearly is failing in its primary task!

On the whole, GPS is a very big win, but you do have to take

every
"recommendation" it gives you with some level of skepticism.
Within the
canyons of Manhattan, the GPS system often thinks that you are
in the middle
of Central park. Also around NYC (and probably many other
places), the GPS
system isn't accurate enough to get you into the correct lane
for turning,
which sometimes means that you get off at the wrong exit or get
onto the
wrong level of the George Washington Bridge. The net result is
that you end
up in New Jersey instead of Manhattan.

✉ **Re: In-car GPS navigation (Scott, [RISKS-24.10](#))**

<"Schatz, Derek P" <Derek.P.Schatz@boeing.com>>

Wed, 23 Nov 2005 11:43:24 -0800

Mike Scott appears to be making issue of something that the GPS
navigator
companies have already clearly avoided liability for. Every
mapping system
I've ever seen warns that map results may not be completely
accurate and
that you need to verify things for yourself. Those of us who
have been
driving for many years have learned the hazards of taking your
eyes off the
road to futz with something inside the car (then again, some
still haven't).
I don't see a risk with the GPS system here, but rather a risk
with the
son's friend's driving abilities. Besides, it takes London
cabbies years to
learn the intricacies of the city's streets (some 400 years of
intricacy) --

how could we expect a GPS system to have that same knowledge?

Now, it might be a different situation if the car had an auto-pilot system relying on that GPS guidance...

Re: In-car GPS navigation (Scott, [RISKS-24.10](#))

<Ian Chard <ian.chard@sers.ox.ac.uk>>

Thu, 24 Nov 2005 09:33:21 +0000

The disclaimers displayed by such systems (including the one I use, Tomtom) aren't just there to get the manufacturers out of trouble. One-way systems change so frequently that there's no reasonable way you could expect a sat nav device to be completely up-to-date. I've been asked to drive through buildings, across fields and against traffic restrictions, but as the driver I have ultimate control and therefore ultimate responsibility.

To misquote the age-old schoolboy admonition, "if a sat nav system told you to jump off a cliff, would you do it?" :)

Ian Chard, Unix & Network Administrator, Systems and Electronic Resources
Service Oxford University Library Services 80587 / (01865) 280587

Re: In-car GPS navigation (Scott, [RISKS-24.10](#))

<"Jack Christensen" <j.christensen@sbcglobal.net>>

Sat, 26 Nov 2005 17:18:48 -0500

I had a friend whose vehicle had a built-in GPS navigation and map system. When you started the vehicle, the first thing on the screen was a disclaimer (which, if I recall correctly, had a fair amount of similarity to that of the Garmin unit.) The unit would not go into operational mode until you touched a button on the screen to "acknowledge" the disclaimer.

At first, I laughed at this, but upon thinking about it a little more, I wasn't so surprised. I am not a lawyer, so I don't know the actual legal worth of this approach, or how it might fare in court.

Jack Christensen, Grand Blanc, MI, USA j.christensen@sbcglobal.net

✉ **Re: UK Police Vehicle Movement Database ([RISKS-24.09](#))**

<Identity withheld by request>
Sun, 20 Nov 2005 9:42:58 PST

The vehicle isn't flagged when the "tax" (Vehicle Excise Licence) is renewed, so this is a misunderstanding of how the system works. The "VEL expired" marker is only added, retrospectively, some time after the renewal falls due, and only if it isn't relicensed as expected. So there is a delay before such a marker is removed following relicensing, but from the foregoing readers can see that a vehicle with an unbroken relicensing

history is therefore never added to the database.

> He then had to spend 5 mins filling in a form as this had to
be regarded
> as an official "stop" event...

Yes, the real value of this is highly questionable (he's fast, if he completed the form in only 5 minutes), and as one stop form has to be completed for each member of a group, you might want to ask your MP if it's a good use of police time to spend up to an hour standing in the street filling in the forms if, say, an officer checks a group of half-a-dozen youths who are the subject of a complaint by a local resident... But that's the reality for officers, and it has been imposed to fulfill a political agenda irrespective of the actual financial cost, the opportunity costs, or the inconvenience to those being spoken to (who, of course, don't actually need to give their details - but the forms still have to be filled in...).

⚡ Re: UK Police Vehicle Movement Database

<mathew <meta@pobox.com>>
Sun, 4 Dec 2005 12:44:29 -0600

> Hence technology + Automation + DVLA = 5 mins wasted police time

It could be worse. In Massachusetts, cities charge you excise tax each year if you own a vehicle.

When you register a vehicle with the Massachusetts Registry of Motor Vehicles (RMV), they inform the city you live in that you have a vehicle and should pay tax.

When you de-register a vehicle--e.g. move to another state, sell the vehicle, return your license plates, and so on--the RMV doesn't bother to inform the city you were in of the new information.

Hence when I bought a car and left Massachusetts permanently, almost a year later I got a completely incorrect tax bill which had been sent to the wrong address. (This was the first I had heard about excise tax, in fact.) MA expected me to pay the incorrect bill and then argue with them to get the money back, or else pay extra non-payment fees. What's more, because they had sent the bill to the wrong address, it had taken so long to arrive I was already subject to non-payment fees.

I can only imagine that this brokenness is deliberate because it monetarily favors the state.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 12

Monday 12 December 2005

Contents

- [Unmanned shuttle system suspended after collision](#)
[Gerrit Muller](#)
- [EFF sues North Carolina over electronic voting-machine certification](#)
[Peter Ludemann](#)
- [A Little Sleuthing Unmasks Writer of Wikipedia Prank](#)
[Katharine Seelye via PGN](#)
- [False WHOIS Data Still Bedevils](#)
[Jim Wagner](#)
- [Miniature Golf Course on Terror Target List](#)
[Paul Saffo](#)
- [Trouble for LAPD computer system](#)
[Dan Laidman via PGN](#)
- [Trading Error Leads to \\$225 Million Loss for Japanese Firm](#)
- [Bulls or bears? Depends on parameter order](#)
[Jeremy Epstein](#)
- [Anti-piracy gone awry in MacInTouch](#)
[Monty Solomon](#)
- [Electronic Switch Fire Exits / Uniform Fire Code](#)
[Daniel Norton](#)
- [Privacy implications of Microsoft's Windows Live Local](#)
[David Pescovitz via Monty Solomon](#)
- [Live Tracking of Mobile Phones Prompts Court Fights on Privacy](#)
[Matt Richtel](#)
- [Letter to Employees about Benefits from Meijer](#)
[James Bauman](#)

- [Re: In-car GPS navigation](#)
[William Ehrich](#)
 - [Re: Y2K++](#)
[Paul E. Ford](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✚ Unmanned shuttle system suspended after collision

<Gerrit Muller <gerrit.muller@gmail.com>>

Thu, 08 Dec 2005 21:30:00 +0100

(From NRC handelsblad, Tuesday December 6, my translation)

The fully automatic, unmanned public transport system Parkshuttle in Rotterdam and Capelle aan den IJssel (in The Netherlands) has been suspended this morning. Two vehicles collided and were severely damaged. According to a spokesman of Connexxion no passengers were present in the shuttles. Connexxion does not have any clue about the cause of the collision. "As long as we don't know that, the shuttles won't ride", according the spokesman. The shuttles are unmanned. They ride on demand and bring passengers from the metrostation Kralingsezoom in Rotterdam to the business park Rivium in Capelle aan den IJssel. Prime minister Balkenende formally started the system last Thursday. The system appeared to have a second youth after a trial period between 1999 and 2001.

Gerrit Muller System Architecting <http://www.gaudisite.nl/>

✚ EFF sues North Carolina over electronic voting-machine certification

<Peter Ludemann <p_ludemann@yahoo.com>>

Fri, 09 Dec 2005 15:25:06 -0800

http://blogs.siliconvalley.com/gmsv/2005/12/babababba_immac.html

So by "independent" you mean "independent of any public oversight," right?

North Carolina is being called to account for its decision to certify electronic voting machines made by three companies that refused to comply with the state's election transparency rules. The Electronic Frontier Foundation (EFF) on Thursday filed a complaint

<<http://www.siliconvalley.com/mld/siliconvalley/13361799.htm>>

against the North Carolina Board of Elections and the North Carolina Office

of Information Technology Services, asking the Superior Court to void the recent "immaculate certifications" they awarded last week

<http://www.eff.org/Activism/E-voting/EFF_Mandamus_Complaint_TRO_20051208140945.pdf>.

North Carolina law requires the Board of Elections to rigorously review all voting system code "prior to certification." But last week the state's Board of Elections certified voting systems from Diebold Election Systems, Sequoia Voting Systems, and Election Systems and Software without bothering to do so (see "Election transparency law damn near invisible

<http://blogs.siliconvalley.com/gmsv/2005/12/so_much_for_nor.html>").

"This is about the rule of law," said EFF Staff Attorney Matt Zimmerman

<http://www.eff.org/news/archives/2005_12.php#004237>.

"The Board of Elections has simply ignored its mandatory obligations under North Carolina election law. This statute was enacted to require election officials to investigate the quality and security of voting systems before approval, and only approve those that are safe and secure. By certifying without a full review of all relevant code, the Board of Elections has now opened the door for North Carolina counties to purchase untested and potentially insecure voting equipment." Keith Long, a North Carolina voting systems manager, defended the state's decision, telling News.com that reports from "independent testing authorities" were sufficient for certification.

<http://news.com.com/EFF+moves+to+block+e-voting+system+certification/2100-1028_3-5988243.html?tag=nefd.top>

But that comes as poor reassurance. Because if the "independent testing authorities" to which Mr. Long refers are as impartial as he is, North Carolina is in big trouble. Long, you see, worked for Diebold Election Systems as recently as Oct. 1, 2004. And between 1983 and 1992 he worked for Sequoia

<<http://www.news-record.com/apps/pbcs.dll/article?AID=/20051113/NEWSREC0101/511130328>>.

Posted by John Paczkowski on 06:46 AM December 09, 2005

🔥 A Little Sleuthing Unmasks Writer of Wikipedia Prank

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

Sun, 11 Dec 2005 17:59:31 PST

John Seigenthaler Sr. (a former editor of **The Tennessean** in Nashville, and founder of the First Amendment Center) was startled to find an entry on himself in Wikipedia that included defamatory false personal information about him -- for example, suggesting that Mr. Seigenthaler had been involved in the assassinations of John and Robert Kennedy. Mr. Seigenthaler then wrote an op-ed article in **USA Today**, noting among other things that he was

especially annoyed that he could not track down the perpetrator because of Internet privacy laws.

The culprit's IP address led to his employer by Daniel Brandt of San Antonio -- who has been a frequent critic of Wikipedia after reading false information about himself! See his www.wikipedia-watch.org.

This led Brian Chase in Nashville to admit having written the offensive material as a joke, stating that he thought that Wikipedia was a "gag" Web site! [Source: Katharine Q. Seelye, *The New York Times*, 11 Dec 2005; PGN-ed]

Coincidentally, that story broke on about the same day that the December 2005 issue of the *Communications of the ACM* came out, the inside back cover Inside Risks column of which is ``Wikipedia Risks''

<http://www.csl.sri.com/neumann/insiderisks05.html>

-- written by four long-time RISKS contributors, Peter Denning, Jim Horning, David Parnas, and Lauren Weinstein who are on my ACM Committee on Computers and Public Policy. This case points up just one of the risks associated with Wikipedia noted in the Inside Risks article, namely that of having an encyclopedia contributed by thousands of volunteers, with few controls on content. PGN

✂ False WHOIS Data Still Bedevils (Jim Wagner)

<"Peter G. Neumann" <neumann@csl.sri.com>>
Sun, 11 Dec 2005 16:23:31 PST

A U.S. Government Accountability Office (GAO) report in Nov 2005 says that there are roughly 2,310,000 Web addresses for which the owner or contact information is unknown. That represents 5% of all .com, .net, and .org domain names. This provides anonymity for spammers, scammers, phishers, and other illegal activities, and untraceability for malware-containing sites. [Source: Jim Wagner, *Internet News*, 8 Dec 2005; PGN-ed]

<http://www.internetnews.com/ent-news/article.php/3569521>

✂ Miniature Golf Course on Terror Target List

<Paul Saffo <pls@well.com>>
Sat, 10 Dec 2005 18:17:29 -0800

Emerald Hills Golfland, in San Jose, California, is a theme park with two

miniature golf courses. It was discovered by San Jose Police to be on a Homeland Security watch list (to prevent it from boarding planes?). Of course, the list is secret. [Source: AP item, 9 Dec 2005; PGN-ed]

<http://www.kron.com/Global/story.asp?S=4226663>

✚ Trouble for LAPD computer system

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

Wed, 30 Nov 2005 6:47:36 PST

A software glitch has interrupted the sweeping overhaul of city emergency communications, which could delay the upgrade of police car computer systems by up to two years, officials said Monday. News about the glitch in the city's \$15 million contract with Northrop Grumman Information Technology drew a strong reaction from the City Council's Public Safety Committee. [Source: Dan Laidman, Glitch triggers outcry on panel; Woes may delay police car computer upgrade, *Los Angeles Daily News*, 29 Nov 2005; PGN-ed; thanks to Lauren Weinstein for contributing this item.]

✚ Trading Error Leads to \$225 Million Loss for Japanese Firm

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

Thu, 1 Dec 2005 13:47:36 PST

Japanese financial-services firm Mizuho Securities Co. said Thursday it erroneously placed sell orders because of a simple human data-input mistake that apparently ignored an error warning. This cost Mizuho at least 27 billion yen (\$225 million). The company mistakenly sold 610,000 shares of J-Com Co. at 1 yen (less than 1 cent) per share, instead of the request to sell just one share at 610,000 yen (\$5,080). The mishap sent the benchmark Nikkei 225 index down 1.95 percent on the Tokyo Stock Exchange. Mizuho Financial Group dropped 3.4 percent to 890,000 yen (\$7,416.67). [Source: AP item, 8 Dec 2005; PGN-ed]

<http://www.timesonline.co.uk/article/0,,3-1917093,00.html>

[Many thanks to Chuck Weinstock, George Mannes, FJReinke, and Tomas Uribe, all of whom sent in the full item. Tomas commented:

One would think that "money-critical" systems would have more stringent safeguards against this type of thing. Also, someone must have made \$225 million as well--who might have been the lucky ones who bought the discounted shares?

PGN]

⚡ Bulls or bears? Depends on parameter order

<Jeremy Epstein <jeremy.epstein@webmethods.com>>

Mon, 12 Dec 2005 14:21:45 -0500

Seems that we don't learn from mistakes (as if that should be a revelation to readers of this list)!

Trouble began Thursday morning, when Mizuho Securities tried to sell 610,000 shares at 1 yen (less than a penny) apiece in a job recruiting firm called J-Com Co., which was having its public debut on the exchange. It had actually intended to sell 1 share at 610,000 yen (\$5,041).

<http://www.washingtonpost.com/wp-dyn/content/article/2005/12/09/AR2005120900087.html>

Also at <http://www.nytimes.com/aponline/business/AP-Japan-Botched-Trade.html> and many other places.

As this problem sounded rather familiar, I searched the RISKS archive, and found it in [RISKS-21.81](#). That posting, almost exactly four years ago, included the following excerpt:

Before the Tokyo market opened Friday, a UBS Warburg trader entered what was intended to be an order to sell 16 Dentsu shares at 610,000 yen (\$4,924.53) each or above. Instead, the trader keyed in an order to sell 610,000 Dentsu shares at 16 yen apiece ...

That was also on the day of a "public debut" (aka IPO). However, it was a bargain - it cost UBS Warburg about \$100M vs. about \$235M for Mizuho Securities.

I assume it's just coincidence that these two failures were both on the Tokyo Stock market.

[I knew the new case sounded familiar! Perhaps the 610,000 is a default number for an erroneous field? That's quite a coincidence. PGN]

⚡ Anti-piracy gone awry in MacInTouch

<Monty Solomon <monty@roscom.com>>

Thu, 8 Dec 2005 01:27:21 -0500

Found on MacInTouch

We received an unconfirmed report that Printer Setup Repair 5.0.3 incorporates a hidden and dangerous anti-copying mechanism, and the company responded to our follow-up with an explanation:

[MacInTouch Reader]

Printer Setup Repair, the widely-used utility for Mac OS X printers, has taken a malicious approach to combatting software piracy. With version 5.0.3 for Mac OS X Tiger, if the user enters a pirated serial number known to the program, the program will immediately and without any warning remove all user preferences and the user keychain, and possibly do other unknown damage to the user's system. [...]

[John Goodchild, President, Fixamac Software, Inc]

Thank you for bringing this to our attention. We have examined our code and discovered an error in the area that rejects pirated registration codes. The original objective was to delete the Printer Setup Repair preferences but a misplaced space in the code allowed the entire user preferences folder to be erased. This would only occur if a pirated code was used. The error was probably overlooked since there was a need to block a new batch of pirated codes quickly. There was no such error in the area that handles legitimate registration codes and in no way can occur if a legitimate registration code is entered incorrectly since the user name is also a part of our internal tests. We have fixed the problem and posted an update. This was not a malicious act on our part, rather an effort to protect our product from software pirates, and we regret any damage that may have been caused by the use of pirated registration codes. Anyone who downloaded Printer Setup Repair 5.0.3 between 11-05-05 and 12-06-05 should download the current release from our web site.

⚡ Electronic Switch Fire Exits / Uniform Fire Code

<"Daniel Norton" <danorton@gmail.com>>

9 Dec 2005 09:39:22 -0800

Is there something in the Uniform Fire Code that addresses electronic switches on exit doors? I work in a building that has two sets of doors towards the exit that both have electronic switches that have failed in several instances.

The first set of doors has a capacitance touch switch which won't work if one is wearing gloves or has a prosthesis. The second set of doors uses a motion detector, which fails if you stand too close to the doors for more than five seconds (you have to subsequently wave at the detector to trigger it).

This seems fundamentally flawed and hazardous. I've just learned that my employer was informed by the Austin Fire Department that touch switches are specifically allowed and they're preferred over motion sensors (which are no longer allowed in new installations).

It doesn't seem to me that someone would naturally know that they need to actually touch a metal bar with their skin in order to exit a door and there have been several instances of fellow employees stalled at the door waiting from someone else to come along and "magically" open the door.

✦ Privacy implications of Microsoft's Windows Live Local

<Monty Solomon <monty@roscom.com>>

Sat, 10 Dec 2005 22:29:20 -0500

Privacy implications of Microsoft's Windows Live Local
David Pescovitz, 9 Dec 2005

Mike Liebhold, my colleague at the Institute for the Future, is deep into the geohacking scene. He just took a look at Microsoft's new Virtual Earth incarnation, Windows Live Local and found some big privacy concerns

[Mike's entire post to the Geowanking listserv on Microsoft's "Location Finder" is online:

http://www.boingboing.net/2005/12/09/privacy_implications.html

PGN]

✦ Live Tracking of Mobile Phones Prompts Court Fights on Privacy

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

Sun, 11 Dec 2005 19:55:01 PST

(Matt Richtel)

Cellular operators know, within about 300 yards, the location of their subscribers whenever a phone is turned on. The operators have said that they turn over location information when presented with a court order to do so. However, in the last four months, three federal judges have denied prosecutors the right to get cellphone tracking information from wireless companies without first showing "probable cause" to believe that a crime has been or is being committed. That is the same standard applied to requests for search warrants. [Source: Matt Richtel, *The New York Times*, 10 Dec

2005; PGN-ed]

<http://www.nytimes.com/2005/12/10/technology/10phone.html?ei=5094&en=4dace02ac3105d11&hp=&ex=1134190800&partner=homepage&pagewanted=print>

[Note: Missouri has granted a contract for statewide cell-phone tracking.]

✈ Letter to Employees about Benefits from Meijer

<"Bauman, James" <James.Bauman@safety-kleen.com>>

Thu, 8 Dec 2005 15:03:23 -0500

My teenaged-daughter works at a Meijer store (<http://www.meijer.com/> -- they have retail superstores in Ohio, Illinois, Indiana, Michigan and Kentucky) near us, and she'd waived any health insurance benefits, because she's covered under my plan.

Recently, she received a letter about the benefit's choices that she'd made. On the first side of the letter is a standard form letter with her name and address and employee number. On the other side of the letter is a detailed accounting of her benefits package. The only problem is that the name on this other side is not hers, and it lists the benefits chosen by another employee from another state with an employee number two digits before hers.

The benefits side of the letter listed the other person's name, address, employee number, home phone, and date of birth, but not a social security number. Because the other person had waived his benefits like my daughter had, there was little information. But, if the person had chosen a benefits package and had decided to cover their dependents, then the following information for the dependents would have been listed: names, relationship, birth date, sex, and social security number.

I called the 1-800 number on the letter about the mistake, and the person that answered immediately said that there's a message about that. I was transferred to a pre-recording. It said that the company was aware that this had affected a lot of their employees, and that employees who'd receive someone else's information are asked to destroy the letters.

I hope their employees do the right and honorable thing, and do not use the identifying information for nefarious purposes, but we all know that the lamp of Diogenes would go out when within a mile of a few people...the ones we all worry about.

Jim Bauman, S-K Lotus Notes Group, 1-847-468-3014 jbauman@safety-kleen.com

⚡ Re: In-car GPS navigation (Scott, [RISKS-24.10](#))

<William Ehrich <ehrich@mninter.net>>

Thu, 8 Dec 2005 12:07:15 -0600

The GPS algorithms include measures of the accuracy and reliability of the current solution. These should be displayed, for instance with an appropriately large fuzz ball on a map display.

⚡ Re: Y2K++ (Horning, [RISKS-24.11](#))

<Paul E. Ford <pef@swcp.com>>

Wednesday, December 07, 2005 2:57 PM

I would conjecture that the list of dates you present are poorly formatted, but correct. Given the rising sequence in the last 2 digits and selective set in the first digit, I would surmise that these represent some sort of quarter data. So, 98Q4 through 05Q3. [...]

Any possibility the second position 0s are actually Qs?

> 4098 3099 2000 1001 4001 4002 2003 1004 4004 3005

[Jim responded:

Paul, What sharp eyes you have! You could see those Qs even when I transcribed the data by hand. I can barely see them as Qs on the original, even given your helpful suggestion, but I do believe that you are correct. Jim H.]

[Also noted by Amos Shapir, who observed that the date labels are placed three quarters apart. But that still does not explain the "4002", which looks as if it should have been "3002". Before running Jim's item in [RISKS-24.11](#), I explicitly asked him to check whether the "4002" was accurately represented by him, and he did verify that. So, I suspect that the "4002" may have been a recording error in the original, or else a lapse in the reporting schedule. 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

Search RISKS using [swish-e](#)

Volume 24: Issue 13

Weds 28 December 2005

Contents

- [Oil blaze hits hospital systems](#)
[Paul Bennett](#) [Pete Mellor](#)
- [The drunks may save our election system](#)
[Danny Burstein](#)
- [Risks of spreadsheets](#)
[Fernando Pereira](#)
- [James Reason on Absent-mindedness and risk management](#)
[James Cameron](#)
- [Yet another leap year error](#)
[Bruce Hamilton](#)
- [Kansas Lottery Picks Same Number Three Nights in a Row](#)
[PGN](#)
- [No one lost or made \\$225 million...](#)
[Bob Heuman](#)
- [Re: A Little Sleuthing Unmasks Writer of Wikipedia Prank](#)
[Ian Halliday](#)
- [Re: In-car GPS navigation](#)
[Gary G. Taylor](#) [Dan Jacobson](#) [Sean Dunn](#) [Alex Colvin](#)

- [Re: False WHOIS Data Still Bedevils
Dag-Erling Smørgrav Dave Bell](#)
 - [Re: Miniature Golf Course on Terror Target List
Rick Jones via PGN](#)
 - [Countering Trusting Trust through Diverse Double-Compiling
David Wheeler via Curt Sampson](#)
 - [REVIEW: "The Art of Computer Virus Research and Defense", Peter Szor
Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Oil blaze hits hospital systems

<Paul.Bennett@jet.uk (Paul Bennett)>

Tue, 13 Dec 2005 17:23:56 -0000

In the light of the Buncefield Oil Depot explosion, we should all consider what local events beyond our control may do to our precious computer and control systems.

A computer system at a Cambridge hospital used for patient information such as admissions and discharges experienced some problems because of a fire at the Buncefield oil depot in Hertfordshire. A company providing some IT services to Addenbrooke's Hospital was based at the industrial park near the depot and was destroyed in the fire. It was expected to take a week to get the computer system up again, although reportedly no medical services were affected. [BBC report; PGN-ed]

Paul E. Bennett, Systems Engineer, UKAEA-JET, Culham Science Centre
Abingdon, Oxon OX14 3DB Tel: 01235-464884

Oil blaze hits hospital systems

<Pete Mellor <pm@csr.city.ac.uk>>

Sat, 17 Dec 2005 17:12:37 +0000 (GMT)

The explosion and fire at the fuel depot near Hemel Hempstead, Hertfordshire:

<http://images.thetimes.co.uk/TGD/picture/0,,250768,00.jpg>

Connection with computers? Well, several nearby installations were wrecked (amazingly, no-one was seriously injured), one of which contained the electronic patient records of Addenbrooke's Hospital, Cambridge. The hospital reported that it would have to rely on paper records for several days until the computer files could be restored.

On the positive side, at least they had back-up. On the other hand, their disaster recovery planning seems to be a bit slack.

Peter Mellor, Centre for Software Reliability, City University, London EC1V 0HB

+44 (0)20 7040 8422 Pete Mellor <p.mellor@csr.city.ac.uk>

The drunks may save our election system (WSJ)

<danny burstein <dannyb@panix.com>>

Fri, 16 Dec 2005 06:59:11 -0500

Fascinating... Per the attached clip from the *Wall Street Journal*, Florida

(FLORIDA!) courts have been agreeing that defendants in "driving while under the influence" cases have a right to full disclosure of the software used in the equipment doing the measuring.

Imagine if this logic followed through to the equipment being slid into election vote counting!

"A court fight in Florida over the software used in the instruments that detect alcohol in breath could threaten the ability of states and localities to prosecute drunk drivers.

"The battle is over the source code of breath analyzers made by CMI Group, a closely held maker of breath-alcohol instruments. Defense lawyers have challenged the use of the device and asked to see the original source code that serves as its computer brain, saying their clients have the right to examine the machine that brings evidence against them.

"Last February, a state appeals court in Daytona Beach ruled that Florida had to produce 'full information' about the test that establishes the blood-alcohol level of people accused of driving under the influence, or DUI. Otherwise, the court said, the evidence is inadmissible...

rest at:

http://online.wsj.com/article_print/SB113470249958424310.html

Risks of spreadsheets

<Fernando Pereira <pereira@cis.upenn.edu>>

Fri, 23 Dec 2005 10:30:58 -0500

Ivars Peterson, The Risky Business of Spreadsheet Errors

Science News, Week of 17 Dec 2005

<http://www.sciencenews.org/articles/20051217/mathtrek.asp>

Spreadsheets create an illusion of orderliness, accuracy, and integrity. The tidy rows and columns of data, instant calculations, eerily invisible updating, and other features of these ubiquitous instruments contribute to this soothing impression. At the same time, faulty spreadsheets and poor spreadsheet practices have been implicated in a wide variety of business and financial problems.

[PGN-excerpted from a nice article with a bunch of references, including

Ivars' 1996 book, *Fatal Defect: Chasing Killer Computer Bugs*, which itself

cited some earlier RISKS reports. The last two references are particularly relevant:

The European Spreadsheet Risks Interest Group (EuSpRIG) has a Web site

at <http://www.eusprig.org/>.

Spreadsheet Research, maintained by Ray Panko of the University of

Hawaii, is a repository for research on spreadsheet development,

testing, use, and technology: <http://panko.cba.hawaii.edu/ssr/>.]

James Reason on Absent-mindedness and risk management

<James Cameron <james.cameron@hp.com>>

Mon, 19 Dec 2005 10:48:49 +1100

Here is an interview that is very suitable for passing on to your non-technical friends who don't understand why you are so morbidly fascinated with risks.

The interviewee is James Reason, Emeritus Professor of Psychology, University of Manchester in the U.K. Professor Reason appears in RISKS a few times (4.52, 10.31, 21.48, 23.24) and is well known for the "Swiss Cheese Model".

The interview was released by the Australian Broadcasting Corporation (ABC) this morning, a repeat from 16th May 2005, and covers;

- * Absentmindedness,
- * the Tenerife disaster (1977, two Boeing 747s collide),
- * no remedial benefit from blame,
- * root cause analysis,
- * the Gimli Glider.

It's available as an MP3 file:

http://abc.net.au/rn/podcast/feeds/health_20051219.mp3

A transcript:

<http://www.abc.net.au/rn/talks/8.30/helthrpt/stories/s1529677.htm>

James Cameron <http://ftp.hp.com.au/sigs/jc/>

Yet another leap year error

<<bruce_hamilton@agilent.com>>

Mon, 19 Dec 2005 13:18:29 -0800

Last month my wife got a CAN 0.03 credit on her Toronto Dominion Visa bill, labelled "Leap year -- interest credit." The note says "The leap year interest credit on your statement is a correction for an over charge in the 2004 leap year."

I don't remember seeing one of these for 2000. Interesting that they would get that right and 2004 wrong.

Incidentally, the bill has our US ZIP code printed with Canadian spacing: "940 25".

bruce_hamilton@agilent.com Tel: +1 650 485 2818 Fax: +1 650 485 1103
Agilent Technologies MS 24M-A, 3500 Deer Creek Road, Palo Alto CA 94303

⚡ Kansas Lottery Picks Same Number Three Nights in a Row

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

Tue, 20 Dec 2005 19:06:59 PST

The same three numbers (5-0-9) came up in the same order on 16, 17, and 18 Dec 2005 in the Kansas Lottery Pick Three. On the third night, many people apparently chose 5-0-9, costing the lottery nearly twice what was paid in. Lottery security officials insist that the system was working normally.

(Perhaps the random-number generator had gone to seed?) [PGN-ed. Thanks to Lauren Weinstein for spotting this one.]

<http://abcnews.go.com/US/story?id=1425383>

✶ No one lost or made \$225 million... (Re: [RISKS-24.12](#))

<RsH <rsh@idirect.com>>

Mon, 12 Dec 2005 21:16:27 -0500

Re: Trading Error Leads to \$225 Million Loss for Japanese Firm

As per the information in the Reuters item

<http://asia.news.yahoo.com/051211/3/2c7vk.html>

the actual loss may be lower or more than the \$225 million as the amount of

the premium that will need to be paid to buy back shares is still to be

determined. The sale order was for about 41 times the actual number of

shares actually outstanding, incidentally.

It turns out that the Tokyo Stock Exchange's own software was responsible

for part of the problem, as it prevented the cancellation of the order from

being processed!

See <http://www.yomiuri.co.jp/dy/business/20051210TDY08010.htm>

which says:

Observers also said the TSE held some responsibility for the incident

because it accepted the unusual sell order. The TSE does not have a

system to automatically detect an unusual order, and the bourse will come

under pressure to remedy this situation.

Also note that this is NOT the first time this has happened at the TSE, and they have yet to fix their system! RSH

[From the same article...]

Incident not without precedent

Thursday's incident was not the first time a large-scale errant order was placed in the nation. In November 2001, UBS Warburg (Japan) Ltd. (now UBS Securities Japan Ltd.) issued an order to "sell 610,000 shares at 16 yen each," instead of "sell 16 shares at 610,000 yen each," for newly listed Dentsu Inc. stock on the First Section of the TSE. It is believed that UBS Warburg incurred significant losses due to this erroneous order. In December of the same year, Deutsche Securities Ltd. made a massive sell order for Isuzu Motors Ltd. stock, but the order was not processed because it was made soon before the market closed. In both cases, the price and amount of shares were inadvertently mixed up.

Note added Mon, 26 Dec 2005:

[More fallout from the error... with a better number on the loss actually suffered.]

Exchange chief resigns over 'fat finger' error, From Leo Lewis in Tokyo

The Times, 21 Dec 2005

<http://business.timesonline.co.uk/article/0,,13133-1948579,00.html>

The president of the Tokyo Stock Exchange resigned yesterday to take

responsibility for the ``fat-finger'' trading error that sparked a day of mayhem on Tokyo markets earlier this month. Takuo Tsurushima resigned along with Sadao Yoshino, the bourse's managing director, and Yasuo Tobiyama, its head of computer systems. The incident has left considerable turmoil in its wake: Mizuho Securities lost 40 billion yen (Â£195 million) on the botched trade and two Japanese day traders made Y2.5 billion in a few minutes.

Western investment houses who made money from the error have been publicly criticised by the Japanese Government and agreed to pay the profits they made into an investors' protection fund.

Losses from the trade were sufficient to force Mizuho to cancel all end-of-year bonuses from the securities arm. The trader, believed to be a 24-year-old woman relatively inexperienced on the dealing floor, had wanted to sell one share in J Com, a new telecoms firm, for Y600,000. She mistyped the order and sold 600,000 shares at Y1 each.

🔥 Re: A Little Sleuthing Unmasks Writer of Wikipedia Prank

<Ian Halliday <ian.halliday@gmail.com>>
Tue, 13 Dec 2005 07:57:33 +0000

The claim that "he thought Wikipedia was a gag site" ([RISKS-24.12](#))

seems unlikely, and I see it on a par with those who say "no, I

was
just doing research" when caught hacking/visiting dubious web
sites.
Yet this seems to have caught the attention of some parts of the
media
who don't usually see visiting those sites as plausible research.
The suggestion is that it is reasonable for somebody to be so
mistaken
as to think Wikipedia is a "gag" site. While some of the
information
there may not be 100% accurate, it's hard to see how this
apparently
mistaken view can be seen as a genuine defence.

Ian W Halliday, BA Hons, SA Fin, ATMG, CL

✉ **Re: In-car GPS navigation (Scott, [RISKS-24.10](#))**

<"Gary G. Taylor" <gary@notdonavan.org>>

Fri, 23 Dec 2005 06:17:05 GMT

Desite the fact that there are many different map atlas programs
for the US
(although this entry concerns UK), they all use the same map
database. Why?
Because there is **only one available,** unless you care to
compile your
own. But this presents problems.

For example: Using **any** map atlas program for the US, tell it
to show you
the intersection of Amboy Road and Wilson Road in Twentynine
Palms, CA.
This is a remote desert area and only Amboy Road is paved ... in
a manner of
speaking. Any of these programs will show a Mercedes-Benz-logo-
shaped triad
of three roads running south from this intersection. Take it

from one who
lived in that area for many years: none of those roads exist.
The database
was compiled from USGS topo maps and the one for that area is
dated (ISTR)
1953, and if you are told to "turn right" at that point and
blindly do you
will piss off a lot of local residents because you will take out
their
mailboxes.

And The Moral Is: Such programs should ALWAYS be taken with a
grain of salt,
even in urban areas. And: The farther from urban areas you get,
the less
reliable these programs are likely to be.

⚡ Re: In-car GPS navigation (Scott, [RISKS-24.10](#))

<Dan Jacobson <jidanni@jidanni.org>>
Thu, 15 Dec 2005 03:38:21 +0800

< if a sat nav system told you to jump off a cliff

Pals armed with my cliff top estate coordinates ended up at the
bottom of
the cliff, and had to pay a local boozer to guide them the
wasted 15 km. to
the top. Moral: X,Y perhaps 100% but without considering Z, your
sat nav
system just gets you into more trouble.

⚡ Re: In-car GPS navigation (Scott, [RISKS-24.10](#))

<"Sean Dunn" <sad14159@hotmail.com>>

Thu, 08 Dec 2005 11:09:47 -0500

Accepting instructions that are reasonably obviously wrong (e.g. one-way streets tend to have signs that indicate the restriction) can be a small problem. Pinpoint lane accuracy can be a problem in specific locations where divergent destinations depend on this accuracy. A harder-to-address problem with GPS navigation can be the reliance upon simple geography...

When I was consulting to IBM in Los Angeles some years ago, one of the team was given a Hertz car with the NeverLost system. Traveling together, we had to ignore its turning suggestion after encountering roadwork and were impressed - a route recalculation showed us the new way to reach the same destination.

We experimented with how clever this system was. And discovered a limitation we had not considered. After heading west back towards LA very late at night, we turned off the freeway and asked the system to see if it could find us a new route to central LA. Alas, the route it chose took us through what could most charitably be called a 'rundown' area. In fact, we were horrified to discover we seemed to have found a route through what we later found out was one of the most dangerous areas in Los Angeles.

GPS systems can hardly be programmed to avoid seedy neighborhoods without political uproar. On the other hand, there are roads that shouldn't be traveled at some times of the day...

⚡ **Re: In-car GPS navigation (Scott, [RISKS-24.10](#))**

<Alex Colvin <alexc@TheWorld.com>>
Tue, 13 Dec 2005 02:01:16 +0000 (UTC)

Note that road coordinates are not known with perfect accuracy either.

Unless someone with a GPS has surveyed the road recently, the coordinates

may have been lifted from a paper map and translated through several datums.

For that matter, driving directions may use outdated one-way and turn

restriction information. This used to be especially obvious in Boston during

the big dig, where the airport exit changed every few weeks.

In the end, it's a lot of fuzz.

⚡ **Re: False WHOIS Data Still Bedevils (Wagner, [RISKS-24.12](#))**

<des@des.no (= ?iso-8859-1?q?Dag-Erling_Sm=F8rgrav?=)>
Tue, 13 Dec 2005 12:32:48 +0100

> ... This provides anonymity for spammers, scammers, phishers, and other
> illegal activities, and untraceability for malware-containing sites.

It also provides relative anonymity for people like paralegal Pamela Jones, who operates groklaw.net, an award-winning web site dedicated to reporting on and analyzing "legal events important to the [Free and Open

Source

Software] community". Her relentless digging into the SCO lawsuits has made her the target of harassment and defamation by SCO and its supporters, such as journalist Maureen O'Gara - ask Google for the sordid details.

Dag-Erling Smørgrav - des@des.no

⚡ Re: False WHOIS Data Still Bedevils (Wagner, [RISKS-24.12](#))

<Dave Bell <zhochaka@gmail.com>>

Tue, 13 Dec 2005 09:38:47 +0000

I just hope that the GAO knows the difference between "unknown" and "withheld". My domain name is registered in the UK, and because of UK and European data protection laws applying to personal data, the WHOIS doesn't return certain information.

⚡ Re: Miniature Golf Course on Terror Target List

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

Tue, 13 Dec 2005 9:25:38 PST

[Rick Jones submitted this comment on the item in [RISKS-24.12](#). Many thanks! PGN]

<<http://www.kron.com/Global/story.asp?S=4226663>>

While the RISKS text talks as if the Golfland was on a

terrorist watch

list as in a list of presumed potential terrorists, a close look at the

text on kron.com shows:

"The moment we realized it was on the list, it was taken off," said San

Jose police officer Rubens Dalaison, who handles "critical infrastructure assessment" for the department. "I myself took it off."

Now, the rest of the text says things like "watch list" which sounds like

the Mr. Smith Will Go to Guantanamo list, however, IIRC the "critical

infrastructure assessment" bit suggests that someone listed the Golfland

as a piece of critical infrastructure, that is as a potential terrorist

target, not as a potential terrorist.

Is the Risk in what KRON published, how it was read by different people,

that a Golfland was on a list in the first place, or all of the above?-))

What is left open is if any of the other Golfland's are considered

critical infrastructure, and perhaps how many people feel that a Golfland

is more critical infrastructure than say Fortress US Capitol...

[I think PGN was in Goofland not Golfland when he PGN-ed the item. PGN]

⚡ Countering Trusting Trust through Diverse Double-Compiling

<Curt Sampson <cjs@cynic.net>>

Fri, 16 Dec 2005 09:24:51 +0900 (JST)

Here is a clear, relatively concise (13 pages) and detailed description and demonstration of a solution to a particular RISK that we're probably all familiar with.

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

Date: Mon, 12 Dec 2005 17:03:54 -0500
From: David A. Wheeler <dwheeler@ida.org>
To: bugtraq@securityfocus.com
Subject: Countering Trusting Trust through Diverse Double-Compiling

Everyone here should be familiar with Ken Thompson's famous "Reflections on Trusting Trust." If not, see:

<http://www.acm.org/classics/sep95/>

The "trusting trust" attack subverts the compiler binary; if attacker succeeds, you're doomed. Well, till now.

I've written a paper on an approach to counter this attack. See:

"Countering Trusting Trust through Diverse Double-Compiling"
<http://www.acsa-admin.org/2005/abstracts/47.html>

Here's the abstract:

"An Air Force evaluation of Multics, and Ken Thompson's famous Turing award lecture "Reflections on Trusting Trust," showed that compilers can be subverted to insert malicious Trojan horses into critical software, including themselves. If this attack goes undetected, even complete analysis of a system's source code will not find the malicious code that is running, and methods for detecting this particular attack are not widely known. This paper describes a practical technique, termed diverse double-compiling (DDC), that detects this attack and some unintended compiler defects as

well. Simply recompile the purported source code twice: once with a second (trusted) compiler, and again using the result of the first compilation. If the result is bit-for-bit identical with the untrusted binary, then the source code accurately represents the binary. This technique has been mentioned informally, but its issues and ramifications have not been identified or discussed in a peer-reviewed work, nor has a public demonstration been made. This paper describes the technique, justifies it, describes how to overcome practical challenges, and demonstrates it."

I think you'll find this interesting.

--- David A. Wheeler

REVIEW: "The Art of Computer Virus Research and Defense", Peter Szor

<Rob Slade <rMslade@shaw.ca>>
Mon, 19 Dec 2005 10:13:23 -0800

BKACVRAD.RVW 20050731

"The Art of Computer Virus Research and Defense", Peter Szor, 2005,

0-321-30454-3, U\$49.99/C\$69.99

%A Peter Szor pszor@acm.org

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8

%D 2005

%G 0-321-30454-3

%I Addison-Wesley Publishing Co.

%O U\$49.99/C\$69.99 416-447-5101 800-822-6339 bkexpress@aw.com

%O [http://www.amazon.com/exec/obidos/ASIN/0321304543/
robladesinterne](http://www.amazon.com/exec/obidos/ASIN/0321304543/robladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/0321304543/
robladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0321304543/robladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/0321304543/
robladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0321304543/robladesin03-20)

%O Audience s+ Tech 3 Writing 2 (see revfaq.htm for explanation)

%P 713 p.

%T "The Art of Computer Virus Research and Defense"

The preface states that the book is a compilation of research over a fifteen year period. While it is not explicitly stated, Szor seems to indicate that the primary audience for the work consists of those professionally engaged in the field of malware research and protection. (He also admits that his writing might be a little rough, which is true. While his text is generally clear enough, it is frequently disjointed, and often appears incomplete or jumpy. Illustrations are habitually less than helpful, although this can't be attributed to a lack of command of English.) Given the stature of people he lists in the acknowledgments one can hope for good quality in the technical information.

Part one deals with the strategies of the attacker. Chapter one describes games and studies of natural ecologies relevant to computer viruses, as well as the early history (and even pre-history) of these programs. I could cavil that he misses some points (such as the 1980-81 Apple virus programs at two universities in Texas), or glosses over some important events (such as Shoch and Hupp's worm experiments at Xerox PARC), but the background is much better and broader than that found in most chronicles. The beginnings of malicious code

analysis are provided in chapter two, although it concentrates on a glossary of malware types (albeit incomplete and not always universally agreed) and the CARO (Computer Antivirus Research Organization) naming convention. The environment in which viruses operate, particularly hardware and operating system platform dependencies, is reviewed in chapter three. This material is much more detailed than that given in any other virus related text. (Dependencies missing from the list seem to be those that utilize protective software itself, such as the old virus that used a function of the Thunderbyte antivirus to spread, or the more recent Witty worm, targeted at the BlackIce firewall. Companion viruses utilizing precedence priorities would seem to be related to operating system functions, but are not included in that section.) Unfortunately, the content will not be of direct and immediate use, since it primarily points out issues and relies on the reader's background to understand how to deal with the problems, but nonetheless the material is fascinating and the inventory impressive. Chapter four outlines infection strategies and is likewise comprehensive. Memory use and infection strategies are described in chapter five. The issue of viral self-protection; tactics to avoid detection and elimination; are given in chapter six. Chapter seven reviews variations on the theme of polymorphism, and also catalogues some of the virus generation kits. Payload types are enumerated in chapter eight. Oddly, botnets are mentioned neither here, nor in the material on worms, in chapter nine. (Szor's use of a modified Cohenesque definition of a virus as infecting files means that some of the items listed in this section are what would otherwise be called email viruses. His usage is

not
always consistent, as in the earlier mention of script viruses
on page
81.) "Exploits," in chapter ten, covers a multitude of software
vulnerabilities that might be used by a variety of malware
categories
for diverse purposes. This content is also some of the best
that I've
seen dealing with the matter of software vulnerabilities, and
would be
well recommended to those interested in building secure
applications.

Part two moves into the area of defence. Chapter eleven
describes the
basic types of antiviral or antimalware programs, concentrating
primarily on various forms of scanning, although change
detection and
activity monitoring/restriction are mentioned. It is often
desirable
to find and disable malware in memory. The means of doing so,
particularly in the hiding-place riddled Win32 system, are
described
in chapter twelve. Means of blocking worm attacks are discussed
in
chapter thirteen, although most appear to be either forms of
application proxy firewalling, or (somewhat ironically) activity
monitoring. Chapter fourteen lists generic network protection
mechanisms, such as firewalls and intrusion detection systems,
although the section on the use of network sniffers to capture
memory-
only worms is intriguing to the researcher. Software analysis,
and
the tools therefore, is covered in chapter fifteen, emphasizing
functional aspects of the malware. Chapter sixteen concludes
with a
register of Websites for further study and reference.

For those involved in malware research, Szor's book is easily
the best
since Ferbrache's "A Pathology of Computer Viruses" (cf.
BKPTHVIR.RVW). It contains a wealth of information found
nowhere else

in book form. On the other hand, it is demanding of the reader, both in terms of the often uneven writing style, and the background knowledge of computer internals and programming that is required. The text does not provide material that would be suitable for general protection of computer systems and networks. On the other hand, intelligent amateur students of malicious software will find much to reward their investigation of this book.

copyright Robert M. Slade, 2005 BKACVRAD.RVW 20050731
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.
niu.edu
http://victoria.tc.ca/techrev or <http://sun.soci.niu.edu/~rslade>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 14

Wednesday 4 January 2006

Contents

- [United airlines computer out/r/age](#)
[Mark Seiden](#)
- [Cat dials 911, saves owner](#)
[Amos Shapir](#)
- [System fakes prisoner releases](#)
[Peter Scott](#)
- [Marriott customer data for 200,000 missing](#)
[Monty Solomon](#)
- [Another calendar error](#)
[Bruce Stein](#)
- [Greenpeace donation transfers accidentally multiplied by 100](#)
[Nick Rothwell](#)
- [PDF documents can leak image data](#)
[Geoff Kuenning](#)
- [Re: The drunks may save our election system](#)
[Tanner Andrews](#)
- [Re: Kansas Lottery Picks Same Number Three Nights in a Row](#)
[Aaron Emigh](#)

- [Re: Double compiling for debugging](#)
[Ken Knowlton](#)
 - [Never write checks on your birthday](#)
[Bob Mehlman](#)
 - [Re: Sat nav systems](#)
[Graham Reed](#)
 - [Expedia doesn't understand phishing](#)
[Art](#)
 - [False positive on check](#)
[F John Reinke](#)
 - [REVIEW: "CyberTerror", R.J. Pineiro](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈ **United airlines computer out/r/age (From Dave Farber's IP)**

<mis@seiden.com>

January 4, 2006 3:55:16 PM EST

What, in this day and age, would cause a complete more-than-5-hour outage of an system mission critical for an airline?

According to AP and Reuters:

"Computer Glitch Delays United Air Flights In US, 3 Jan 2006
United Airlines' domestic flights were delayed up to 90 minutes Tuesday night because of an outage in the computer system controlling United's check-ins and reservations, which went down for about five hours around 5 p.m. CST Wednesday. Passengers were checked manually, and flights were delayed up to 90 minutes. [PGN-ed]

But according to me, who was at LAX yesterday trying to get to

Oakland at
5pm on their one-and-only flight, the outage was complete and
system-wide.

* No self-check-in kiosks working, reservationists answering the
phone with
"our computers are still down", which meant every queue had more
than 500
people in it, spilling out on the sidewalk outside the terminal,
and they
were using "the manual procedure". the people close to the head
of the
queue had been waiting for more than two hours, they said, and
they
dispensed with the special queues for premier or 1k, just to
spread the pain
equally.

* They weren't calling out specific flights to try to fill them.

* They had most of the check-in desks empty. Obviously they
don't have
enough people trained in the manual procedure to alleviate the
bottleneck.

* The woman working the lines (with a megaphone) was apologetic,
but
wouldn't answer questions, not even frequently asked questions
which did not
have to with individual problems, such as "if I miss my last
flight will you
provide a hotel? or is my ticket now refundable if I fly
another carrier?"

* some reports are they were flying planes half-empty because
people
couldn't get to the gates. of course, they weren't announcing
how long they
were holding flights to try to board them.

* TSA, not known for their flexibility, was not allowing people
to go to the
gates directly with a boarding pass. Even an e-ticket receipt

with a seat
assignment wouldn't get you there.

United stock is down 2% today, trading at around a buck a
share. their
earnings are -\$43 per share at the moment. I'll bet this was an
expensive
failure.

(As for me, I scooted right over to Southwest, and got out only
1.5 hours
later, but buying a one-way last minute ticket guarantees you'll
get the
dreaded four ssss "special screening" on your boarding pass.)

[IP Archives: [http://www.interesting-people.org/archives/
interesting-people/](http://www.interesting-people.org/archives/interesting-people/)]

⚡ Cat dials 911, saves owner

<"Amos Shapir" <amos083@hotmail.com>>
Wed, 04 Jan 2006 16:23:00 +0200

See details in <http://www.msnbc.msn.com/id/10663270/?GT1=7538> .
(I think
there was a similar report on RISKS a few years back, that time
about a
dog).

[Yes. For example, The risks of Canadian Poodles using 911,
[RISKS-15.70](#).

PGN]<corrected in archive>

⚡ System fakes prisoner releases

<Peter Scott <risks@psdt.com>>

Sat, 31 Dec 2005 17:07:05 -0800

The RISKS archives include several cases of prisoners being erroneously released by errant computer systems. This might be the first case of a system that only pretended to release them. CNN reports at <http://us.cnn.com/2005/LAW/12/31/inmate.scare.ap/index.html> that an automated notification system at the Ohio Department of Rehabilitation and Correction telephoned about 3,000 people the day before New Year's Eve to inform them of the recent release of a prisoner that had victimized them or a family member. Unfortunately - or fortunately, depending on how charitable you are - that wasn't the truth. The prisoners had not been released but were listed in a file accidentally sent to the contractor that handled notifications. No word on whether the size of that file was unusually large.

⚡ Marriott customer data for 200,000 missing

<Monty Solomon <monty@roscom.com>>

Wed, 28 Dec 2005 23:10:33 -0500

The timeshare unit of Marriott International Inc. is notifying more than 200,000 people that their personal data are missing after backup computer tapes went missing from a Florida office. The data relates to 206,000 employees, timeshare owners and timeshare customers of Marriott Vacation

Club International, the company said in a statement Tuesday. The computer tapes were stored in Orlando, where the unit is based.

The company did not say when the tapes disappeared. They contained Social Security numbers, bank and credit card numbers, according to letters the company began sending customers on Saturday. ... [*The Boston Globe*, 28 Dec 2005]

http://www.boston.com/business/articles/2005/12/28/marriott_customer_data_for_200000_missing/

⚡ Another calendar error

<Bruce Stein <bruce42@pacbell.net>>
Thu, 29 Dec 2005 18:59:22 -0800 (PST)

Go to <http://www.protopage.com> . This is a free site where you can design a home page for yourself. There is a calendar in the upper right hand corner. Hover your cursor on it and it will change to a full calendar for the current month. Use the left arrow on this calendar to go back one month. Continue doing this until you get to January, 2001. Then go back one more time. You are now in December 3900. (!)

⚡ Greenpeace donation transfers accidentally multiplied by 100

<Nick Rothwell <nick@cassiel.com>>

Thu, 29 Dec 2005 23:11:50 +0000

Approximately 10000 UK supporters of Greenpeace who make regular donations by direct debit have have accidentally had their bank accounts debited by a hundred times their usual amount, with its software adding two noughts to the latest batch of direct debit demands.

<http://news.bbc.co.uk/1/hi/uk/4567944.stm>

I would hazard a guess that some manual intervention was made, perhaps to update the records for a new calendar year, leading to a mistake by a real human being rather than "the computer."

nick rothwell <http://www.cassiel.com>

[A different kind of environmental hazard,
the Greenpeace dreadnought strikes again. PGN]

PDF documents can leak image data

<Geoff Kuenning <geoff@cs.hmc.edu>>

04 Jan 2006 02:09:06 -0800

A colleague recently provided me with a PDF of a presentation he created using Keynote on a Macintosh. I needed to use some photographs from that document in a presentation of my own, so I used pdfimages, a public-domain tool, to extract them. Imagine my surprise when I discovered several images that were not apparent in the original, including logos for Yahoo and MSN, a

snapshot of a commercial Web page, and a photograph of some former students.

I have not experimented with random files from the Web, so I don't know what tool is responsible for inserting the inadvertent images in the file, although it seems to be a classic case of using an existing document as a template for a new one. Clearly, however, PDF documents are capable of carrying images that are not visible to the casual user, and thus risk leaking information in the same way as Microsoft Word and Powerpoint.

Geoff Kuenning geoff@cs.hmc.edu <http://www.cs.hmc.edu/~geoff/>

[For example, see [RISKS-23.86](#)-88 for the discussion on using PDF to redact classified documents. PGN]

✶ Re: The drunks may save our election system ([RISKS-24.14](#))

<tanner andrews <tanner@payer.org>>
Thu, 29 Dec 2005 09:43:06 -0500 (EST)

db-) [if drunk drivers an see code, why can't voters?]

** First, let me be clear that I am not a lawyer. This
** is a political opinion piece, not legal advice.

Distinguish the drunks, who are entitled by law to ``full information'',
State v. Muldowny and Pitts, 871 So.2d 911 (Fla. 5DCA 2004)
(discussing Fla. Stat. 316.1932(1)(f)(4)), from the voters who have no obvious similar

entitlement.

1. Muldowny and Pitts prevailed under a theory that they had a right to discovery in their respective criminal cases. The court agreed, criticizing the box as ``a mystical machine'' in the absence of source: it simply inhaled breath samples and spat out a report of guilt.

The burden in a criminal case is on the state to show that the machine was certified. Because the firmware is an essential component of the machine (perhaps the single most important, and easiest to change), they were entitled to see the code and verify that it was as certified. Failing that, of course, you can have a ``Wizard of Oz'' effect, where the man behind the curtain presses a secret button and the machine says ``drunk''.

2. Voter cases are different. They obviously cannot rely on a discovery theory as in Muldowny because the ptf's would not be charged with any crime. Standing can probably be had by having an affected voter file a protest; a losing candidate would be the obvious ptf. However, the barrier is that the ptf must have knowledge of actual fraud, and must swear to it.

This gives rise to a chicken-and-egg problem. How is the voter to know of the fraud without inspecting the machine? And how is the voter to gain access to inspect the machine, absent knowledge of fraud?

The Muldowny defs attacked the certification of the machine, in part. The statute required that the machine be certified, Muldowny at 913 (discussing Fla. Stat. 316.1932(1)(a)), and material changes would require new certification. The defs wanted to show that the machine as

used was not
the same as was certified.

The voter ptf will have to show that the use of uncertified
equipment
affected the outcome. Courts are reluctant to overturn
elections.

Beckstrom v. Canvassing Board, 707 So.2d 720 (Fla. 1998) (gross
negligence,
but no fraud, so affirming result preserving election); Boardman
v. Esteva,
323 So.2d 259 (Fla. 1975).

Following Beckstrom, the ptf will have to show actual fraud in
the
handling of the votes in order to prevail. This will be a
higher hurdle
than it might appear. In Beckstrom, the supervisor of
elections allowed
Vogel supporters to ``correct'' ballots that were incorrectly
marked for
Beckstrom. This was held to be gross negligence but not fraud.

I would expect that a pre-load, as was demonstrated in Leon,
might qualify
as actual fraud. A pre-load is where one sets the number of
votes for one
candidate to +N and for the other to -N, such that the total is
still zero.
The negative count rolls over, of course, during the course of
the day.

3. An alternative theory is to attack under Fla. Stat. 119.07
(Public
Records law). Ballots are inspectable as public records, though
the
conditions of inspection are onerous. It could be argued,
though likely
without success, that the machines' guts are public records as
well.

A public record is (1) a record (2) made or received (3) during
the course

of official business. Adv. Op, David Wagner re: Legal Bills, Fla. AGO-2000-7; Shevin v. Bryan, 379 So.2d 633, 640 (Fla. 1980).

Certainly the ballots qualify on all elements.

It seems likely that the machines are made or received during the course of official business. But do they qualify as records?

The supervisor of elections never receives the source code, and I do not believe that the Department of Elections does either. It is hard to see it as a public record on that basis.

Could we at least see the machine code? I don't think this theory works, either: if it did, we could all have a copy of Windows for the cost of reproduction, assuming they use the same at City Hall.

If that theory works, how about embedded devices? Could we require the road department to open up and let us dump the code out of computer-based surveying equipment?

The essential quality of being ``a record'' is missing in these cases. The machine code in the voting machine, or in the desktop computer, or in the surveying equipment, is not a record: it is not the preservation and transfer of knowledge. It is more analogous to the power steering arm of a car: it is there to perform a function, not to convey knowledge; the engineering knowledge embedded in it is there only for the purpose of accomplishing the function.

Accordingly, I would not expect a Public Records attack to open up the

source for the machines.

4. The analysis changes if the device uses any GPL code. In such a case, delivery of the device necessarily implies delivery of the object code, and the licensing terms require that copies of the source be made available to anyone to whom the object is given.

The Supervisor of elections would be entitled, under the GPL, to the source code of a machine using GPL code in its deliverables.

An entity cannot defeat public records inquiry by reposing custody in a third party. *Times v. St Pete*, 558 So.2d 487 (Fla. 1990). The interested person may go to the Supervisor's office and require that a record of that office be produced. Such an attack seems likely to prevail, though the litigation may be expensive and time-consuming.

5. It seems unlikely that a voter could use `_Muldowny_` to open up the code to black box voting machines. Nor is a general public record challenge likely to work, unless the machine uses GPL code.

[Re: Kansas Lottery Picks Same Number Three Nights in a Row \(R-24.13\)](#)

<"Aaron Emigh" <aaron-risks@radixlabs.com>>
Wed, 28 Dec 2005 19:44:08 -0800

The article in [RISKS-24.13](#) states that "The odds of winning the lottery are

one in 1,000. The probability that the numbers will be the same three nights in a row are a staggering one in a billion." This is off by three orders of magnitude.

Of course, the odds of drawing the digits 5-0-9, or any other specific combination, three nights in a row are one in a billion with an honest random number generator. But we don't care what number is drawn the first night. For a three-peat, we require only that that first night's number, whatever it is, be drawn again twice. The odds are one in a million, not one in a billion. The observed sequence is a curious fluke, but not entirely implausible for a properly functioning random number generator. Many improbable properties can be found in nearly any large dataset...

[Also noted by George Kaplan. PGN]

⚡ Re: Double compiling for debugging (Wheeler, [RISKS 24.13](#))

<Ken Knowlton <KCKnowlton@aol.com>>

Thu, 29 Dec 2005 10:34:29 EST

David Wheeler's comments on double compiling ([RISKS-24.13](#)) bring to mind a paper of mine, "A Combination Hardware-Software Debugging System," *IEEE Trans. Computers*, C-17, 1, Jan 1968, pp 84-86. Briefly:

Two versions of a program, logically identical, have sections of program

and data mapped differently into memory; storage is initialized with the same sequences of "random" numbers. The programs are run synchronously.

The hardware knows which parts of instructions and data -- including data

to be overwritten -- should match, and complains when they don't. Several

kinds of error are thus detected close on the heels of misbehavior.

[There is nothing knew under the son of the farther... PGN]

⚡ Never write checks on your birthday

<rmehlman@jumpy.igpp.ucla.edu>

Fri, 30 Dec 2005 19:56:43 -0800 (PST)

You'll get the year wrong...

...and may not even notice, since you've written your date of birth

so many times. (Well, it's a risk of the human computer.)

⚡ Re: Sat nav systems (Dunn, [RISKS-24.13](#))

<Graham Reed <greed@pobox.com>>

Tue, 03 Jan 2006 15:18:10 -0500

"Sean Dunn" <sad14159@hotmail.com> writes:

> GPS systems can hardly be programmed to avoid seedy neighborhoods without

> political uproar. On the other hand, there are roads that shouldn't be

> traveled at some times of the day...

However, the newer-generation of aftermarket units, at least those from Garmin, can be provided with both rectangular and road-based "avoidances" loaded at the user's request. In Garmin's case, the avoidances can be used for on-computer route planning with older units, but not for route planning or re-calculating on the unit itself.

So, although it would be politically wrong for the GPS makers to pre-load such data, user groups could collude to fill in the gap, and provided down-loadable files that can be used to set up the programmed avoidances on the GPS units. At least, the ones that can be programmed by your PC in the first place.

Mind you, this raises a new RISK of people seeding the database with bad data for other reasons: keeping folks away from competing businesses, for example. But that's not really new, downloading untrusted data from the Internet is a RISK as old as the 'net itself.

GPS is a case of a technology that works more than well enough in general, that it is very easy to forget its limitations. Right up until the time you're looking at a muddy gravel road on your heavy sport-touring motorcycle because the road was supposed to have been paved, but the budget was cut so the work was never done....

[Of course, map makers always seed their maps with a few intentional errors to be able to spot ripoffs. PGN]

✈ **Expedia doesn't understand phishing**

<art-risks@dontsharemyemail.com>

Thu, 29 Dec 2005 09:36:57 -0500

I use a unique email address for things I sign up for online so that I can track email leakages.

The other day I received an email to my expedia email from usmail@expediamail.com - a domain that pops up a blank page in my browser. It was offering some wonderful offer if I just clicked on an encoded link that went to expediamail.com.

Q: In this day and age of phishing, how retarded does a company have to be to use a domain that is similar, but different, from its own domain to send out "wonderful offers" from?

A: As retarded as only Microsoft can be apparently. I wrote to Expedia and they confirmed that they use that address to send out promotional offers. They told me how to stop receiving them, but when I went to set my preferences to not get them, they were already set to not get them. So apparently Expedia doesn't even adhere to their own members' preferences.

When I asked about that, they said "yes, you aren't signed up to receive the offers, maybe someone else did it (after having confirmed that they did it), here's how you turn off receiving offers..."

The risks are losing potential customers by sending out emails

that look
like phishing expeditions

⚡ False positive on check

<"F John Reinke fjr@anywhere" <reinkefj@yahoo.com>>
Sun, 1 Jan 2006 12:35:42 -0500

The person operating the cash register told [Dan] Ring his account had been flagged for some reason, and he might want to contact his bank.

[Excerpt from Bruce Mohl, **The Boston Globe**, 1 Jan 2006]

Here's an example of Type 1 error - rejecting a good check thereby losing the retailer a sale. Of equal interest should be the approval of a bum check. It appears that the reporter really didn't dig. I wonder where the bodies are buried. It's usually found by following the money trail. Since the retailer doesn't know the customer, they probably don't value the sale properly. I know from the "publisher's free offers", that the repeat business from a satisfied customer is worth a premium. In this case, if the retailer loses the sale and the chance for repeat business, then that indeed is an expensive rejection. Hmmm?

http://www.boston.com/business/globe/articles/2006/01/01/check_verification_system_is_vulnerable_to_mistakes/?rss_id=Boston.com+%2F+Business+%2F+Personal+Finance+-+Money+Management+-+Financial+Management+-+Boston.com

[The article points out that less than a half percent of \$790

billion

point-of-sale checks are erroneously rejected by a system that decides in

about a third of a second whether a check might be bogus. PGN]

⚡REVIEW: "CyberTerror", R.J. Pineiro

<Rob Slade <rMslade@shaw.ca>>

Tue, 27 Dec 2005 20:44:23 -0800

BKCBRTER.RVW 20050929

"CyberTerror", R. J. Pineiro, 2003, 0-765-34304-5

%A R. J. Pineiro author@rjpineiro.com

%C 175 Fifth Avenue, New York, NY 10010

%D 2003

%G 0-765-34304-5

%I Tor Books/Tom Doherty Assoc.

%O pnh@tor.com www.tor.com

%O <http://www.amazon.com/exec/obidos/ASIN/0765343045/>

[robsladesinterne](#)

<http://www.amazon.co.uk/exec/obidos/ASIN/0765343045/>

[robsladesinte-21](#)

%O <http://www.amazon.ca/exec/obidos/ASIN/0765343045/>

[robsladesin03-20](#)

%O Audience n- Tech 0 Writing 1 (see revfaq.htm for explanation)

%P 493 p.

%T "CyberTerror"

Now, those who follow this series will know that, in my opinion, most of the

hype over cyberterrorism is a) overblown, and b) looking at the wrong things

anyway. However, this book goes beyond the norm. It reminds me of that old

joke about the difference between a used car salesman and a computer

salesman being that the used car salesman knows when he is lying to you.

All right, let's look at what he got right. Yes, computers do control a lot of "infrastructure." Yes, the worst disasters are when there are multiple (and usually cascading) failures in both control and safety systems. Yes, developers, maintainers, and even service people do leave trapdoors in systems. And, yes again, if you were going to perform terrorist acts, it would be best to target a number of interrelated systems.

Now, before we look at the technical problems, a few practical ones. The advantage of cyberterrorism is said to be that you can, from the comfort of your own (remote and safe) hacienda, blow up your enemy's city with a few keystrokes. The terrorists in this book must be pretty unskilled, because they seem to need money, traitors, advance information, bomb materials--in short, everything that any other terrorists need when they are doing noncyberterrorism. (The characters aren't terribly consistent: for example, we have one Middle Eastern terrorist who reverts to Hispanic at moments of stress.)

As for the technology, it isn't good. We have the usual movie-script-oriented virtual reality interface, completely ignoring the realities of internal computer operations, and the fact that providing complicated forensic information via a simple graphical interface would be a very difficult task indeed. (Oh, and we also have the famous, mythical

"digital-pulse-bomb-that-gets-from-the-computer-into-your-head-and-gives-you-a-stroke" program.) Pineiro contradicts himself, telling us that there is a virus, then that there is no evidence of a virus (the mythical "undetectable" virus: a virus *always* changes *something*), and then that there is a virus. (The author never defines what a virus is, which, given how much else he gets wrong, is probably a good thing. Supposedly a virus can be used as traceroute, a RAT, a trojan, or anything you want.) While it was a big deal fifteen years ago, a T1 carrier is hardly high-speed anymore, particularly between related companies. As a devotee of software forensics, I approve of the fact that characteristics of a computer system can be used to gain information about the user, but I hardly think it boils down to a choice of pink defensive software for girls and blue for boys.

Pineiro does not seem to know the difference between computer hardware and computer software. (We have, of course, already seen that computer software can generate sufficient power to fry circuitry, and even people.) Programs (some of which can be as small as two bytes long) communicate via certain frequencies, like radio signals. When you stop the system clock, somehow memory locations begin to lose charge. (No, I don't think he is referring to the fact that DRAM needs to refresh every millisecond or so.) The author also doesn't seem to realize that, regardless of what language was used to write the original program, most software in production systems tends to be object code. (He also seems to think that you can stop the

system

clock and thus halt programs originally written in Ada, but leave programs originally written in C still running.)

With their magical virtual reality interface, the blackhats never seem to need to know what system they are attacking. It's got some UNIX-like characteristics, but that blue screen just has to be Windows. Which is too bad, given that most embedded systems tend to be specialized hardware, and not subject to any off-the-shelf malware. (As of the mid-90s, most nuclear power plants still used PDPs, keeping at least one plant running turning out replacement parts for them.)

Pineiro also displays his ignorance of artificial intelligence. Despite his "neural-like" type of expert system program that amalgamates all known AI techniques, a neural net is one approach to AI, while an expert system is quite a different one. Not all AI systems are capable of learning: in fact, it's quite a feat to put learning capability into a package. (And I love the "Turing Society": I'm sure that those in Turing's home country of Britain would be thrilled to have the US defence department deciding who can, and can't, mess around with their AI programs. The implication of the Society is rather Frankensteinish, although Hans Moravec, in "Robot: Mere Machine to Transcendent Mind" [cf.BKRBTMMT.RVW], would probably agree with the possibility of AI taking over, if not the necessity of inhibiting it.)

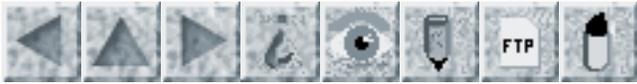
Cyberterrorism is certainly possible, and a lot of systems should be

protected more rigorously than they are at present. However,
this book
provides no feeling for the realities of cyberterrorism--or
anything else,
for that matter.

copyright Robert M. Slade, 2005 BKCBRTER.RVW 20050929
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.
niu.edu
http://victoria.tc.ca/techrev or [http://sun.soci.niu.edu/
~rslade](http://sun.soci.niu.edu/~rslade)



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 15

Saturday 28 January 2006

Contents

- [Google's Search Query Log vs. China Censoring: Perceptions Matter!](#)
[Lauren Weinstein](#)
- [NSA on redacting Word and PDF documents](#)
[dmagda](#)
- [NTSB report on Southwest Airlines crash](#)
[Joe Thompson](#)
- [United computer failure](#)
[Steve Wildstrom](#)
- [H&R Block blunder exposed SSNs](#)
[Leigh Blankenship](#)
- ["Analog Hole" Bill to impose secret requirement?](#)
[Randall](#)
- [NSA explains how to redact documents electronically](#)
[Steven M. Bellovin](#)
- [Phone calling records for sale instantly](#)
[Lauren Weinstein via PGN](#)
- ['Hacker' held over U.S. Navy breach](#)
[Bob Heuman](#)

- [Bank loses tape with personal information on 90,000 customers](#)
[John Christoffersen via Monty Solomon](#)
 - [Re: Bank loses tape with personal information on 90,000 customers](#)
[Dan Shoop](#)
 - [Another finger goof at the Tokyo Exchange, Lower loss, wrong company!](#)
[Bob Heuman](#)
 - [E-mail and the courts](#)
[Art T.](#)
 - [Cisco, haven't we learned anything?](#)
[Gadi Evron](#)
 - [REVIEW: "Rootkits", Greg Hoglund/James Butler](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

🔥 Google's Search Query Log vs. China Censoring: Perceptions Matter!

<Lauren Weinstein <lauren@vortex.com>>
Thu, 26 Jan 2006 17:39:19 -0800 (PST)

Reality matters, but perceptions can matter even more.

The juxtaposition of Google's stance on the Feds' search query log COPA data demand and Google's decision to cooperate with China's censorship does not realistically represent "hypocrisy" as is being erroneously suggested by various media articles. The two issues are very different in many key aspects.

However, this is not to minimize the enormous risks to Google -- and other Internet services -- if they're perceived to be making "inconsistent" policy decisions that directly affect important issues (often relating

to essentially non-technical impacts) about which many people are very concerned, and often very emotional.

Now, as was completely predictable, Congress is getting involved.

Congressman Tim Ryan has announced a hearing of the Congressional Human Rights Caucus (16 Feb is the date that I've heard) to explore the potential drafting of laws that would limit or otherwise control U.S.-based Internet companies from complying with the censorship demands of foreign countries. Emotions were clearly exasperated by Google's launching of the "dot-cn" Chinese version of Google search that blocks links as per Chinese government directives, though Google is not alone in this regard among U.S.-based Internet companies.

Ryan also specifically tied this to the COPA case, directly and dramatically suggesting that Google was more willing to obey Chinese law than U.S. law. This is an example of the perception risk I described above crystalized in a very potent way.

The situation highlights the minefield of issues that Google and other Internet companies now face, and the desperate need for proactive approaches to dealing with the ways that these technologies affect individuals and society.

Google's participation in the Chinese censorship program (which I consider to be extremely problematic) creates a perception that is undermining what I view as Google's correct decision regarding the search query COPA case, with

the sorts of reactions we're now seeing.

Coincidentally, I spent a very pleasant afternoon two days ago at Google's Los Angeles (actually Santa Monica) facilities giving a talk regarding exactly these and other issues. This included (among other topics) discussion both regarding those areas where I feel that Google is doing a terrific job, and their policies and operations about which I've been (sometimes highly) critical -- where I feel that changes would be of benefit to Google, their users, and society at large. (Google invited me and we scheduled this talk prior to the breaking of the COPA search query story -- talk about timing...)

I much appreciated the opportunity to address such issues directly at Google and meeting a bunch of nice folks at the site. The talk was taped and I hope that the video will become publicly available in the near future -- I'll let you know.

Lauren Weinstein +1-818-225-2800 <http://www.pfir.org/lauren>
<http://lauren.vortex.com> <http://daythink.vortex.com> lauren@pfir.org

🔥 NSA on redacting Word and PDF documents

<dmagda@ee.ryerson.ca>

Sat, 21 Jan 2006 10:23:42 -0500 (EST)

There have been numerous cases in past RISKS issues where

information has
been leaked via electronic documents. This includes mainly the
history
included with Word files and "redacted" PDF files.

It seems that this has finally caught the attention of the US
National
Security Agency (from [1]):

Section 2: Procedures to Sanitize a Word Document

The following steps were tested with MS Word 2000 and Acrobat
5.0 and 6.0.

Other recent versions should work similarly. While time-
consuming, these
steps give the highest confidence that sensitive information is
not hidden
in the released document. Copying the text and images into a
blank document
is a good way to manually review a sensitive document, since
sections can be
copied over one at a time as they are reviewed.

Found via Boing Boing [2].

[1] <http://www.fas.org/sgp/othergov/dod/nsa-redact.pdf> (670 KB)

[2] http://www.boingboing.net/2006/01/21/nsa_howto_sanitize_w.html

NTSB report on Southwest Airlines crash

<Joe Thompson <joe@orion-com.com>>

Fri, 27 Jan 2006 16:12:18 -0500

The NTSB has reported on the cause of the Southwest Airlines
crash in
Chicago:

<http://www.cnn.com/2006/TRAVEL/01/27/airplane.landings/>
<http://www.chicagotribune.com/news/local/chi-060127midwayaccident,1,3064315.story?coll=chi-news-hed>

Executive summary: the thrust reversers did not deploy properly, causing the plane to overshoot the end of the runway.

A point of contention right after the accident was that the pilots had apparently activated the automatic brake system in violation of Southwest policy, but the NTSB concluded the crucial factor was the unanticipated 18-second delay in the thrust-reversers deploying. As a result, NTSB is urging the FAA to prohibit allowing for thrust-reversers in onboard stopping-distance calculations. (Before landing, the crew had used the onboard computer to calculate stopping distance for "wet-poor" conditions; those calculations assumed the thrust reversers would deploy normally.)

The risks here appear to be two of the most common ones: trusting an automatic system to activate within specification 100% of the time, and allowing that trusted system to be the critical margin between success and catastrophic failure -- even in the successful-landing scenario represented by the onboard computer's figures, the plane was anticipated to stop within 30 feet of the end of the runway after a rollout of over 4000 feet, a margin of error of less than 1%. -- Joe

Joe Thompson | joe@orion-com.com

✈ **United computer failure**

<"Steve Wildstrom" <steve_wildstrom@wdc.exchange.businessweek.com>>

Thu, 5 Jan 2006 09:49:58 -0500

More than reservations was affected. I was on a United flight at Dulles waiting to take off at the time the reservation system went down. I was listening to air traffic control when the pilot of my flight and another UAL plane told the tower they couldn't take off because they didn't "have their numbers." Later, our pilot came on the PA and said that because of a computer outage, UAL operations was having to do load and balance computations manually.

Steve Wildstrom, Technology & You columnist, BusinessWeek

✈ **H&R Block blunder exposed SSNs (From Dave Farber's IP)**

<leigh blankenship <leigh_b@mac.com>>

January 5, 2006 3:08:01 PM EST

Happy New Year, 234-56-7890! Trust us and our software to protect your confidential tax information!

http://netscape.com.com/H38R+Block+blunder+exposes+consumer+data/2100-1029_3-6016720.html

> Some consumers may be dismayed to find their Social Security numbers
> printed on unsolicited packages from H&R Block, the result of a recent

> labeling blunder at the company.
>
> The packages, which H&R Block mailed in December, contained
free copies of
> the company's tax preparation software, TaxCut. By mistake,
some of the
> packages also displayed recipients' Social Security numbers,
which were
> embedded in 47-digit tracking codes above mailing labels.

IP Archives at: <http://www.interesting-people.org/archives/interesting-people/>

⚡ "Analog Hole" Bill to impose secret requirement? (via Dave Farber's IP)

<Randall <rvh40@insightbb.com>>
January 24, 2006 5:38:44 PM EST

[First seen on the Telecom Digest]:
http://htdaw.blogspot.com/post.mhtml?post_id=198659

Monday January 23, 2006 by Ed Felten

If you've been reading here lately, you know that I'm no fan of the Sensenbrenner/Conyers analog hole bill. The bill would require almost all analog video devices to implement two technologies called CGMS-A and VEIL. CGMS-A is reasonably well known, but the VEIL content protection technology is relatively new. I wanted to learn more about it.

So I e-mailed the company that sells VEIL and asked for a copy of the specification. I figured I would be able to get it. After all, the bill

would make compliance with the VEIL spec mandatory -- the spec would in effect be part of the law. Surely, I thought, they're not proposing passing a secret law. Surely they're not going to say that the citizenry isn't allowed to know what's in the law that Congress is considering. We're talking about television here, not national security.

After some discussion, the company helpfully explained that I could get the spec, if I first signed their license agreement. The agreement requires me (a) to pay them \$10,000, and (b) to promise not to talk to anybody about what is in the spec. In other words, I can know the contents of the bill Congress is debating, but only if I pay \$10k to a private party, and only if I promise not to tell anybody what is in the bill or engage in public debate about it.

Worse yet, this license covers only half of the technology: the VEIL decoder, which detects VEIL signals. There is no way you or I can find out about the encoder technology that puts VEIL signals into video.

The details of this technology are important for evaluating this bill. How much would the proposed law increase the cost of televisions? How much would it limit the future development of TV technology? How likely is the technology to mistakenly block authorized copying? How adaptable is the technology to the future? All of these questions are important in debating the bill. And none of them can be answered if the technology part of the bill is secret.

Which brings us to the most interesting question of all: Are the members of Congress themselves, and their staffers, allowed to see the spec and talk about it openly? Are they allowed to consult experts for advice? Or are the full contents of this bill secret even from the lawmakers who are considering it?

<http://www.freedom-to-tinker.com/?p=958>

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

<"Steven M. Bellovin" <smb@cs.columbia.edu>>

January 24, 2006 4:01:02 PM EST

Subject: NSA explains how to redact documents electronically
(via Dave Farber)

<http://www.fas.org/sgp/othergov/dod/nsa-redact.pdf>

One wonders how long it will be till someone finds an error...

--Steven M. Bellovin, <http://www.cs.columbia.edu/~smb>

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

Phone calling records for sale instantly (via Lauren Weinstein)

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

Thu, 12 Jan 2006 10:03:05 PST

FBI Agent's Cell Phone Records For Sale Locatecell.com seems to have a good thing going. According to this Chicago Sun Times story:

To test the service, the FBI paid Locatecell.com \$160 to buy the records for an agent's cell phone and received the list within three hours, the police bulletin said.

Representatives of Data Find Solutions Inc., the Tennessee-based operator of Locatecell.com, could not be reached for comment.

Frank Bochte, a spokesman for the FBI in Chicago, said he was aware of the Web site.

"Not only in Chicago, but nationwide, the FBI notified its field offices of this potential threat to the security of our agents, and especially our undercover agents," Bochte said.

Funny how the FBI's first reaction is to go on the defensive. Funny how this is a big surprise to the FBI.

The Chicago Sun-Times paid \$110 to Locatecell.com to purchase a one-month record of calls for this reporter's company cell phone. It was as simple as e-mailing the telephone number to the service along with a credit card number.

Locatecell.com e-mailed a list of 78 telephone numbers this reporter called on his cell phone between Nov. 19 and Dec. 17. The list included calls to law enforcement sources, story subjects and other Sun-Times

reporters and
editors.

Cheating spouse? Disloyal employees? Need to find out what your
competition
is doing? Hey, no problem. Telecom services are just information
services
these days.

Fortunately friend Chris Hoofnagle, of Electronic Privacy
Information
Center, is on the case.

Thanks to Steve Crandall, who spotted this story first!

'Hacker' held over U.S. Navy breach

<Bob Heuman <rsh@idirect.com>>

Mon, 16 Jan 2006 18:05:57 -0500

Of course, not answered [nor likely to be answered] is why the
security even
could be breached at a facility that handles nuclear submarines.
RSH

An 18-year-old suspected Spanish hacker who allegedly breached
the
top-secret computer security of a U.S. Navy base in San Diego
has been
arrested in his home town of Malaga, Spain, according to the
Spanish Civil
Guard. He reportedly "seriously compromised the correct
operations and
security of a maintenance dry dock for nuclear
submarines." [Source: CNN
Madrid Bureau Chief Al Goodman, 16 Jan 2006; PGN-ed]

Bank loses tape with personal information on 90,000 customers

<Monty Solomon <monty@roscom.com>>

January 12, 2006 2:21:39 AM EST

By John Christoffersen, AP Business Writer | January 11, 2006

STAMFORD, Conn. --A tape containing the Social Security numbers and other confidential data of 90,000 People's Bank customers was lost recently while en route to a credit reporting bureau, state and bank officials said Wednesday.

Millions of people around the country have been affected by a recent string of data losses and thefts involving major financial institutions and businesses including Citigroup Inc., Time Warner Inc. and Ameritrade Holding Corp.

People's has no reason to believe the data has been used inappropriately and has received no reports of unauthorized activity, officials said. Customers do not need to close accounts because the information is not sufficient to allow unauthorized access, the bank said.

But consumer advocates say identity thieves could use Social Security numbers to open new accounts in the names of those affected.

They say such data should be encrypted so it cannot be illegally accessed and they advocate new laws that would allow consumers to place fraud or security alerts on their credit reports to prevent thieves from

creating
accounts. ...

http://www.boston.com/news/local/connecticut/articles/2006/01/11/bank_loses_tape_with_personal_information_on_90000_customers/

Re: Bank loses tape with personal information on 90,000 customers

<Dan Shoop <shoop@iwiring.net>>
January 12, 2006 9:41:01 AM EST

(From Dave Farber's IP)

This actually happens all the time. The bank FedEx's or otherwise sends a tape, it get's lost. This happens. In a past life as a datacenter manager at Citibank we used to receive palettes of tapes by FedEx every morning from Sioux Falls, SD, where the credit card processing center was, a truck of tapes having better bandwidth at lower cost than any telco line. Occasionally tapes got lost, it was no big deal and no one thought much of it other than to request another copy. California, IIRC, was the first state to mandate that any lost customer records of any sort has to be reported, and other states have followed suit. Since such laws been enacted that it must be reported it's been getting recent press and what is actually a common occurrence is now "news". The risk from this is considered very low. In most all cases the data is encrypted. Even if it wasn't other policies prevent keeping say account numbers and names, or other

required
pieces of information necessary to commit a fraud or identity
theft with
information together in the same place at once.

Having names and Social Security numbers together is considered
low risk
since this information is readily available through numerous
sources.

Dan Shoop, Systems & Networks Architect 1-646-217-4725
<http://www.iwiring.net/> <http://www.ustsvs.com/> shoop@iwiring.net

Another finger goof at the Tokyo Exchange, Lower loss, wrong company!

<Bob Heuman <rsh@idirect.com>>
Fri, 13 Jan 2006 20:24:55 -0500

A Japanese trader pushed the wrong button Friday and cost his
brokerage
house almost 500 million yen, or \$5.1 million Cdn. The incident
is the
latest in a series of blunders and computer glitches on the
Tokyo Stock
Exchange, Japan's biggest bourse. In the latest case, a trader
with Daiwa
Securities SMBC apparently made a mistake just before the start
of trading
and sold 25,000 shares of the wrong company. Daiwa realized the
error a few
minutes later and issued a buy-back order, but investors had
already snapped
up 13,000 shares. The brokerage house repurchased all those
shares by the
end of the trading day, but lost almost 500 million yen (\$5.1
million Cdn)
in the process, according to Daiwa spokesman Daishu Nagata.

[Source:

Trader's typing error costs Japanese brokerage house millions

CBC News, 13

Jan 2006; PGN-ed; see [RISKS-24.12](#) for the earlier Mizuho screwup.]

<http://www.cbc.ca/story/business/national/2006/01/13/goof-060113.html>

✶ E-mail and the courts

<"Art T." <myspamtrap01@yahoo.com>>

Wed, 18 Jan 2006 20:29:46 -0500

Here's a site RISKS users might be interested in. It appears to be a

compendium of legal cases in which e-mails play a significant role. It

includes several cases where deleting e-mail has cost companies large

amounts of money, even when the e-mails were not recovered.

<http://arkfeld.blogs.com/ede/email/>

✶ Cisco, haven't we learned anything? (technician reset)

<Gadi Evron <ge@linuxbox.org>>

Thu, 12 Jan 2006 22:19:28 +0200

In this (<http://www.cisco.com/warp/public/707/cisco-sa-20060111-mars.shtml>)

recent Cisco advisory, the company alerts us to a security problem with

Cisco MARS (Cisco Security Monitoring Analysis and Response System).

The security issue is basically a user account on the system that will give you root when accessed.

The account is:

1. Hidden.
2. Default.
3. With a pre-set password.

In other words, this is a journey back 10 years when technicians would commonly have special keys (actual keys, electronics or passwords) to access a device if they have to troubleshoot it for anything, or say? the user lost his password.

People used to trade these keys online and hidden accounts were a thing of common practice. Today people still trade commonly used default passwords but it is not as popular as it used to be, at least in the online world.

On the other hand, the most common practice to hack routers today, is still to try and access the devices with the notoriously famous default login/password for Cisco devices: cisco/cisco.

Cisco/cisco is the single most used default password of our time. It got more routers pwned than any exploit in history, and it still does. One would think that a company such as Cisco, especially with this history, would stay away from such "default" accounts? but the fact that this account is hidden makes it something different.

It makes it a backdoor. One much like those used by the Bad Guys.

Now... if Cisco knowingly put it there, shame on them. If somebody put it there without their knowledge... well, shame on them.

This is indeed a vulnerability, as in a weakness. It is not however a software coding bug that may result in say... a buffer overflow. It is a part of the design of the system. Cisco disclosing this is very nice and commendable, but perhaps they should also let us know whether this was indeed a backdoor somebody put in their system or if it was part of the design?

I love easter eggs. I just don't like surprises in system privileges or backdoors, especially not in a security monitoring and response product.

I very much doubt it was anything else but a part of the design but that should be admitted to. As the advisory states:

"No other Cisco products are currently known to be affected by this vulnerability."

Okay, but how about other vulnerabilities of this type? Are there any more backdoors to other Cisco products? If not, why wouldn't they just come out and say that? "There are NO other such backdoors in our products."

I'd even be happy with: "To our knowledge, there are no other vulnerabilities of this type in our products."

This is not a bug. One can never be sure ALL bugs are eliminated - however hard one may try. One CAN admit to having no such features in

other
products, though.

Once again we fall upon re-naming of a feature as a bug or a bug
as a
feature to make the problem sound less severe.

In this case, the judgment is plain and simple:
If Cisco were Bad Guys, this is a backdoor.
As Cisco are Good Guys, this is a technician reset.

Terminology? What's the difference?

The difference is that Cisco are not Bad Guys. If they
disclosure a
problem they should do it fully, because as a client, I am now
concerned.

This reminds me of Ciscogate but not for obvious reasons. That
was a bad
event for everybody involved.

It reminds me of the very issue Mike Lynn discussed:
Remote exploitation for Cisco is possible, while so far Cisco
disclosed
all these problems as DoS vulnerabilities.
I am not saying Cisco did that on purpose, but in THIS case they
CAN set
my mind at ease.

Why don't they?

Update: After writing this I've been made aware that this
product was from a
company Cisco bought not so long ago. This very same issue
happened before
(and more than once)... in one recent example with another
company Cisco
bought named Riverhead. Checking into new investments security-
wise,
especially with security products and external QA may help solve
such issues
in the future.

REVIEW: "Rootkits", Greg Hoggund/James Butler

<Rob Slade <rMslade@shaw.ca>>

Mon, 09 Jan 2006 07:59:12 -0800

BKROOTKT.RVW 20051023

"Rootkits", Greg Hoggund/James Butler, 2006, 0-321-29431-9,
U\$44.99/C\$62.99

%A Greg Hoggund

%A James Butler

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8

%D 2006

%G 0-321-29431-9

%I Addison-Wesley Publishing Co.

%O U\$44.99/C\$62.99 416-447-5101 fax: 416-443-0948 bkexpress@aw.
com

%O [http://www.amazon.com/exec/obidos/ASIN/0321294319/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0321294319/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/0321294319/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0321294319/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/0321294319/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0321294319/robsladesin03-20)

%O Audience s+ Tech 3 Writing 2 (see revfaq.htm for
explanation)

%P 324 p.

%T "Rootkits: Subverting the Windows Kernel"

The preface (and therefore the book) begins with a definition of a rootkit.

The authors proceed to outline their initial interest in the phenomenon, and any security professional who understands the centrality of system internals can begin to see the importance of the work.

Chapter one addresses a major selling point (in the blackhat

mindset) for rootkits: the evasion of detection. Concentrating on this aspect, the material outlines what a rootkit is, and is not, noting also that the programs need not be limited to illegal activities but do have legitimate uses. Subversion of the core of the operating system is examined in chapter two, although this is limited to the creation of device drivers. (This chapter again raises the issue of whether a book investigating the breaking of a system can provide valuable advice when it comes to protecting computers. While some works do; Hoglund, along with Gary McGraw, having created an example in "Exploiting Software" [cf. BKEXPLSW.RVW]; this particular material concentrates on items of interest in the process of producing rootkits. The limited sections dealing with more theoretical considerations would be those of greater interest to the security community.) Chapter three explores some hardware related items, although there are others that could be perused, and most of those surveyed may be initiated in hardware, but operate primarily in the software realm.

Hooking of interrupts and functions is covered in chapter four, at both a kernel and user level. Chapter five reviews various means of directly patching software. (Much of this material should be familiar for those who have studied operations of older viruses.) The interception techniques addressed in chapter four are extended, in chapter six, to include adding new "layers" to existing device drivers. The operating system kernel uses

data and other resources in order to perform properly, and chapter seven shows that manipulating these objects can modify the actions of the machine. Although nominally about hardware, chapter eight really concentrates on the patching of firmware. Chapter nine examines covert channels, but the explanation is quite poor, and most of the space is dedicated to listings of program code. Rootkit detection is discussed in chapter ten. It is interesting to note that analogies of antiviral change detection and activity monitoring are mentioned, but there is no consideration of signature scanning.

"Rootkits" does raise a number of interesting topics, and much of the material could be of use to those charged with protecting systems. However, the content is not as valuable as that presented in "Exploiting Software." There is, of course, much that will be of assistance for those writing legitimate rootkits, but this would be a fairly limited audience.

copyright Robert M. Slade, 2005 BKROOTKT.RVW 20051023
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.niu.edu
http://victoria.tc.ca/techrev or <http://sun.soci.niu.edu/~rslade>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 16

Weds 15 February 2006

Contents

- [Ameriprise's stolen laptop had data on 230,000 PGN](#)
- [Another example of missing plausibility checks: \\$8M tax bill
Jeremy Epstein](#)
- [Video of my "Internet and Empires" talk at Google
Lauren Weinstein](#)
- [E-mail glitch hides \\$3.98 billion in Air Force deals
Scott Peterson](#)
- [New U.S. grant system excludes Mac users
Rick Weiss](#)
- [Hacker attacks on Danish websites
Klaus Brunnstein](#)
- [A List of Spreadsheet Errors
Gene Wirchenko](#)
- [Re: "NSA on redacting Word and PDF documents"
Matt Jaffe](#)
- [Re: "NTSB report on Southwest Airlines crash"
Peter B. Ladkin \[dwikstrom\]\(#\)](#)

- [Gary McGraw on Software Security](#)
[PGN](#)
 - [REVIEW: "Information Security: Principles and Practice", Mark Stamp](#)
[Rob Slade](#)
 - [REVIEW: "Ending Spam", Jonathan A. Zdziarski](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Ameriprise's stolen laptop had data on 230,000

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

Sun, 29 Jan 2006 20:35:47 PST

Ameriprise Financial said that lists containing the personal information of about 230,000 customers and advisers had been compromised. A security breach occurred in late December 2005, after a company laptop was stolen from an employee's parked car. The laptop contained a list of reassigned customer accounts that was being stored unencrypted, and treated in violation of various Ameriprise rules. [PGN-ed from *The New York Times*, 26 Jan 2006]

[Thanks to Doug McIlroy for spotting this one. Doug remarked on the bad (but seemingly very common) practice, and noted that "a scapegoat has been sacrificed for the company's sins." Also, Bob Heuman cited an item

<http://ct.eneews.eweek.com/rd/cts?d=186-3144-17-83-67263-367596-0-0-0-1>

that gave the number of affected clients as 158,000. PGN]

✦ Another example of missing plausibility checks: \$8M tax bill

<Jeremy Epstein <jeremy.epstein@cox.net>>

Sat, 11 Feb 2006 08:14:43 -0500

AP is reporting that a house in Valparaiso, Indiana (a town of moderately priced homes) received an \$8 million tax bill on a house actually worth \$121,900, but appraised at \$400 million. This sort of thing isn't unusual, but there were some interesting wrinkles:

1. The change in value was made by a person not authorized to make changes.
2. The value change occurred because the person typed one incorrect letter to access the assessment change application (R-E-R vs. R-E-D to perform the intended action)
3. The assessment change application was (theoretically) no longer in use, having been replaced by a newer version
4. Since tax rates are set as a function of the total assessed value of the property in the community (and an extra \$400 million was enough to seriously throw off calculations in this locality), the local government is now significantly short of income, and is laying off staff.

This is a great example of a cascading failure - if any one of these steps hadn't occurred (or had a cross-check - such as an audit trail that detected the use of the old assessment program), the problem would not have occurred.

The county treasurer says that his office noticed & fixed the error, but somehow it propagated elsewhere too.

Article at <http://www.cnn.com/2006/US/02/10/overpriced.house.ap/index.html>

🔥 Video of my "Internet and Empires" talk at Google (1/24/06)

<Lauren Weinstein <lauren@vortex.com>>

Fri, 10 Feb 2006 08:22:30 -0800

A little over two weeks ago, I was invited to Google's Los Angeles area facilities in Santa Monica to give an informal talk ("Internet and Empires") on a range of Internet-related topics. Video of that presentation is now available, and since it touched on a large number of our favorite discussion issues in RISKS, I thought it might be of some interest here.

The topics naturally included a number of the controversial issues related to Google, but also more generally privacy, free speech, ISPs, data retention, government and legal issues, censorship, network neutrality, and more.

The talk ran about an hour and the video will reportedly become available soon as one of Google's "Tech Talks" (<http://video.google.com/videosearch?q=Google+techtalks>).

Since the video is not currently online there (and for people who need or prefer other video formats), I have a Windows Media version available now (my thanks to Google for providing me with a video master for processing).

Please note that all of the opinions expressed in this talk of course are mine, and should naturally not be construed to represent the views of Google, Inc.

Video:

<http://www.vortex.com/lauren-google-2006-01-24.wmv> (Download / ~36MB)

<http://www.vortex.com/lauren-google-2006-01-24.asx> (Streaming)

Audio Only (MP3):

<http://www.vortex.com/lauren-google-2006-01-24.mp3> (MP3 Audio / ~15MB)

Lauren Weinstein lauren@vortex.com lauren@pfir.org <http://www.pfir.org/lauren>

International Open Internet Coalition - <http://www.ioic.net> +1 (818) 225-2800

E-mail glitch hides \$3.98 billion in Air Force deals

<Scott Peterson <scott4@mindspring.com>>

Tue, 14 Feb 2006 13:29:27 -0800

The U.S. Air Force said a new employee's e-mail error kept the Pentagon and the public in the dark about nearly \$4 billion of its contracts in December.

The DoD addresses were dropped from e-mail about more than \$1.57 billion for

Northrop Grumman Corp., \$1.22 billion for Boeing Co. and almost \$509 million

for Lockheed Martin Corp., involving remotely piloted Global Hawk aircraft

and F-22A fighter jets among other contracts. The Defense Department is

supposed to announce each business day at 5 p.m. EST contracts valued at \$5

million or more for its units, including the armed services.

[Source: Jim

Wolf, Reuters, 14 Feb 2006; PGN-ed]

<http://cwflyris.computerworld.com/t/296929/664274/9136/0/>

✦ New U.S. grant system excludes Mac users (Rick Weiss)

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

Mon, 13 Feb 2006 16:49:00 -0500 (EST)

A new U.S. federal government system Grants.gov already costing tens of

billions of dollars over its five-year development cycle is intended to be

used for all grant applications submitted to NIH, Housing and Urban

Development, and 24 other grant-giving agencies, typically giving out

something like \$400B per year. However, its scheduled widespread use will

be postponed because the Windows-based software is not Mac-compatible. In

the interim, some applications will require proposals to be submitted from

MS systems. One blogger is quoted: "this would be the same government that

spent a lot of time and money pursuing Microsoft for its anti-competitive

behavior?" [Source: Rick Weiss, *The Washington Post*, 13 Feb 2006; PGN-ed]

<http://www.washingtonpost.com/wp-dyn/content/article/2006/02/12/AR2006021200942.html?referrer=emailarticle>

⚡ **Hacker attacks on Danish websites**

<"Klaus Brunnstein" <brunnstein@informatik.uni-hamburg.de>>

Thu, 9 Feb 2006 10:59:54 +0100

According to the largest Danish newspaper, Jyllands Posten (known for having first published 10 drawings related to end religion founder Mohammed, in September 2005), the number of attacks on Danish websites esp. for smaller enterprises and private owners raised 10-fold, with more than 900 websites affected in one week.

<http://www.jp.dk/itogc/artikel:aid=3546652/>

(edition: Thursday February 9, 2006)

The "simple forms of attacks" (details not given) were accompanied with pro-Muslim statements esp. against publication of Mohammed drawings.

Btw: evidently, Jyllands Posten's website is still alive, although some access problems have been reported when the issue was reported in worldwide news (probably shortage of bandwidth).

[This is not surprising. However, I think RISKS will stay out of the ensuing brouhaha as being not computer related. PGN]

⚡ **A List of Spreadsheet Errors (Re: Art T, [RISKS-24.15](#))**

<Gene Wirchenko <gene@abhost.us>>

Sun, 29 Jan 2006 16:06:51 -0800

Re: E-mail and the courts

> ... compendium of legal cases in which e-mails play a significant role.

> <http://arkfeld.blogs.com/ede/email/>

And here is one where spreadsheets have caused trouble.

<http://www.eusprig.org/stories.htm>

✉ Re: "NSA on redacting Word and PDF documents" (Magda, [RISKS-24.15](#))

<Matt Jaffe <jaffem@erau.edu>>

Sun, 29 Jan 2006 13:10:02 -0700

What to me seems an obvious risk was not mentioned, namely the risk of trusting untrusted software to perform downgrade at all, regardless of the parameterization (e.g., Track Changes disabled) and combination of operations (deletion, overlay, copy) performed. The COMPUSEC field has known and published for decades that software that can downgrade must be trusted and, of course, running on a TCB trusted to the necessary extent as well. Microsoft has perhaps made some progress in the realm of trusted software in the last few years but I doubt that Word or Windows yet meets anyone's notion of highly trustworthy. Curious, I went to one of the references cited, NSA Report # I333-015R-2005, Redacting with Confidence: How to Safely Publish Sanitized Reports Converted From Word to PDF

<http://www.fas.org/sgp/othergov/dod/nsa-redact.pdf>

There was a caveat included there to the effect that, "Using original source formats, such as MS Word, for downgrading can entail exceptional risks; the lengthy and complicated procedures for mitigating such risks are outside the scope of this note." Well and good (although it's not the format per se that is the problem but the software that processes it and the TCB it executes on), but there were no references provided in the NSA report to additional sources discussing the inherently "exceptional" risk of relying on untrusted software for downgrade operations, no matter how detailed and convoluted and (one hopes) well tested the redaction operations are.

I still think we're misleading people with these band-aid approaches. In the original RISKS article, for example, dmagda states, "these steps give the highest confidence that sensitive information is not hidden in the released document." I don't know why dmagda feels that these techniques provide "highest confidence". Perhaps he or she merely meant that there's nothing better around and these steps are better than nothing. But do they really provide much in the way of confidence in the overall safety of the process? Only to the extent that one trusts Word and Windows to be free of undisclosed Trojan Horses. To not at least more clearly highlight that fact and provide a reference to further literature is a shortcoming in the cited NSA report and the risk is that people may naively assume that since the NSA has published it, it can be relied on with "highest confidence".

✈ **Re: "NTSB report on Southwest Airlines crash" (Thompson, [R-24.15](#))**

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>
Tue, 31 Jan 2006 23:27:37 +0100

Joe Thompson suggested in [RISKS-24.15](#) that the NTSB has "reported on the cause of the Southwest Airlines crash in Chicago" (SWA 1248, Chicago Midway airport, 8 Dec 2005).

The NTSB has not reported on "the cause", and probably will not do so for a while (it is likely that there are many causes, not just one. I see at least four from the facts known so far. See below). The investigation is still under way. The NTSB has released a recommendation, A-06-16, concerning the means of calculating landing distances on contaminated runways. I recommend reading A-06-16 at http://www.nts.gov/Recs/letters/2006/A06_16.pdf

The aircraft landed on a snow-contaminated runway at MDW and overran the runway. It went through a blast fence and onto a public road, where it collided with two cars and killed a young child in one of them.

The pilots had used an "on-board laptop performance computer (OPC)" to calculate landing distances to determine whether they could land at MDW in the snow-stormy conditions. The crew inputted weather data and entered

runway braking conditions as "WET-FAIR" in the OPC. The OPC calculated that the airplane would be able to land and completely stop with 560 feet of runway remaining. However, "the OPC is programmed to assume that the engine thrust reversers will be deployed on touchdown" and they were not so deployed. They deployed 18 seconds after touchdown. "If the reverse thrust credit had not been factored into the stopping distance calculations made by the OPC, it would have indicated that a safe landing on runway 31C was not possible under a braking condition of either fair or poor" (op. cit. p3).

In other words, an implicit assumption made by the OPC program led to the OPC indicating to the pilots that they could land safely on runway 31C when, under the conditions that actually obtained during the landing, the OPC program would have indicated that they could not do so without overrunning.

The reasons for the delayed deployment of reverse thrust have not yet been publicly determined by the Board.

I have pointed out before in this forum (e.g. [RISKS-24.03](#)) that, although the supposedly safety-critical computer systems on commercial aircraft have not yet been implicated in any accident during 18 years in service, the supposedly non-safety-critical computer systems have been causally involved in many fatal accidents. This accident appears to be yet another example.

The four causes obviously indentifiable so far are: the weather conditions,

the OPC calculation that led the crew to believe that they could land safely on 31C, the crew's decision to land on 31C, and the delayed deployment of reverse thrust. And here we can already see part of the reason why these supposedly non-safety-critical computer systems can continue to be relatively so deadly. There is a crew decision and action interposed between the computer actions (in this case, informational output) and the fatal result. Somehow, we allow greater chances of systems misleading a crew into taking fatal actions than we do that the airplane behaves differently from that which is expected from the crew's control inputs.

Put like this, it is hard to see what may justify such apparently incompatible attitudes. But when one looks at the development, it is easier to see how the anomaly comes about. The OPC is probably a much more useful and convenient tool than the paper performance charts which it replaces. There is a legally-blessed principle called GAMAB in France and MGS in Germany which says that one may use a (sub)system B as a replacement for a (sub)system A when one can demonstrate that, in all circumstances of deployment, the risk of using A is at least as great as the risk of using B (usually phrased in terms of the safety of B being at least as great as the safety of A, but "safety" here means the inverse of risk, and there is lower likelihood of misunderstanding if one phrases the principle using the word "risk".) The OPC likely was taken to satisfy the GAMAB/MGS principle in comparison with the paper-based performance charts.

Note that, for all we know so far, the accident could well have

happened

even if the assumption of immediate reverse-thrust had been explicit; for example, the crew had been using paper charts on which the assumption of immediate thrust reverse had been printed. The NTSB focused on the pernicious assumption, not on the means by which it entered the calculation.

Peter B. Ladkin, University of Bielefeld, Germany <www.rvs.uni-bielefeld.de>

Re: "NTSB report on Southwest Airlines crash" (Thompson, [R-24.15](#))

<dwikstrom@lycos.com>

Sun, 29 Jan 2006 21:50:36 -0500

IMO the conclusion of "automatic" Thrust-Reverser failure is premature -- and probably totally inaccurate.

There is yet no reported evidence that the aircraft Thrust-Reversers malfunctioned at all.

Human error by the pilot, not failure of an "Automatic" system -- is the likely cause of late deployment of the Thrust-Reversers in that Chicago, Boeing 737 accident.

The NTSB merely stated that the aircraft flight-recorder showed the Thrust-Reversers deployed 18-seconds after touchdown. There was no statement of actual or suspected failure of the Thrust-Reverser system ---

only later
than expected activation during landing.

The pilot should have 'manually' activated Thrust-Reversers at touchdown.

NTSB also states: "During post-accident interviews, the captain stated that he attempted to immediately deploy the thrust reversers but that he was unable to do so. According to the first officer, at some point during the rollout, he noticed that the thrust reversers were not deployed, and he then reached over and deployed them.."

Since pilot-error is generally the primary cause of any & all aircraft accidents -- IMO it's quite likely the captain failed to deploy Thrust-Reversers... because the co-pilot easily did so, shortly afterward.

Perhaps in hindsight the captain honestly believes he "attempted" to deploy the Thrust-Reversers ... or maybe he's now is trying to cover his error by an alleged system malfunction ??

Note that the NTSB has issued neither a preliminary or final report -- only an advisory related to flight planning & Thrust-reversers ... so full details are unavailable. Newspaper reports tend to blur important considerations in summarizing the NTSB advisory.

Here's the only NTSB reference:

http://www.nts.gov/Recs/letters/2006/A06_16.pdf

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

Sun, 29 Jan 2006 20:35:47 PST

Gary McGraw: Software Security: Building Security In
Addison-Wesley, 2006
ISBN: 0-321-35670-5

This book is a "hands-on, how-to guide for software security" for software security professionals. It completes a trilogy together with McGraw's Building Secure Software (Addison-Wesley, 2001) and Exploiting Software (Addison-Wesley, 2004), but it also stands alone as a useful book. It considers best practices for software security in detail, as a fundamental part of the development lifecycle. It is very much in the spirit of what RISKS has promulgated in the past 20.5 years.

REVIEW: "Information Security: Principles and Practice", Mark Stamp

<Rob Slade <rMslade@shaw.ca>>

Wed, 15 Feb 2006 08:16:42 -0800

BKINSCPP.RVW 20051112

"Information Security: Principles and Practice", Mark Stamp,
2006,
0-471-73848-4

%A Mark Stamp stamp@cs.sjsu.edu

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 2006

%G 0-471-73848-4

%I John Wiley & Sons, Inc.

%O U\$74.95/C\$96.99 416-236-4433 fax: 416-236-4448
%O [http://www.amazon.com/exec/obidos/ASIN/0471738484/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0471738484/robsladesinterne)
[http://www.amazon.co.uk/exec/obidos/ASIN/0471738484/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0471738484/robsladesinte-21)
%O [http://www.amazon.ca/exec/obidos/ASIN/0471738484/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0471738484/robsladesin03-20)
%O Audience i+ Tech 3 Writing 2 (see revfaq.htm for
explanation)
%P 390 p.
%T "Information Security: Principles and Practice"

The preface stresses that the material in this book is intended to provide not only the formal concepts for security, but also advice for the real world. Security is addressed overall, but the work concentrates on cryptography, access controls, and software issues. (The author also adds a discussion of protocols. It is hard to see this as a separate issue, rather than simple implementation details of the other concepts.) The audience is not explicitly stated, but both security professionals and the idea of using the volume as a course text are mentioned.

Chapter one is an introduction. Stamp will strike a very sympathetic chord with many support and security people when he adds a requirement to the normal list of security questions: can the system survive "clever" users? A set of problems are given at the end of the chapter. In contrast to the usual "reading checks," these are thoughtful items, intended to determine if the reader has understood the underlying concepts, and to start discussion.

Part one addresses cryptography. Chapter two provides the

basics, outlining some terms, theory, and history. Functions and algorithms of symmetric key cryptography are explained in chapter three, including some discussion of the controversy over the National Security Agency's role in the development of the Data Encryption Standard. (Stamp points out the weaknesses in the conspiracy theory. It is worth noting that Stamp used to work for the NSA :-)

There are some fascinating additions to the usual material for this topic. Asymmetric algorithms and concepts, again with some interesting notes, are given in chapter four. Chapter five deals with hash functions and related topics (and also has a brief mention of steganography). Advanced cryptanalytic attacks are outlined in chapter six. (Those wanting to pursue this topic *will* have to brush up on their math.)

Part two looks at access control. Chapter seven provides a reasonably complete look at direct authentication issues and technologies. The material on authorization, in chapter eight, extends the normal view of that topic by pointing out the advantages of capability lists and the fact that our basic security models are actually those of authorization. However, Stamp also includes some technologies, such as firewalls and intrusion detection systems, that have only a tenuous connection to authorization.

Part three examines protocols. Chapter nine discusses simple authentication schemes, most relying on some kind of challenge-response system and encryption of some type. Although the writing is clear (and

even amusing), Stamp dives into mathematics, sometimes at crucial moments and without fully explaining the base concepts. For real world security protocols, chapter ten looks at SSL (Secure Sockets Layer) and Kerberos, and also examines IPsec and GSM in some depth, pointing out the weaknesses in design.

Part four deals with software. Chapter eleven explains buffer overflows and other attacks, and also discusses malware. (Stamp makes a rather odd mistake in calling the third type of malware detection "anomaly detection" rather than the more usual activity monitoring. However, the definition of the term fits activity monitoring properly.) Tamper resistance and software testing are legitimately part of software security, but chapter twelve also deals extensively with digital rights management (DRM) which seems to apply more to data protection. The DRM theme is extended in chapter thirteen which addresses operating system security functions, but also discusses Microsoft's upcoming Next Generation Secure Computing Base, which many feel is more applicable to DRM than any real security needs.

An appendix provides an overview of networking, particularly TCP/IP, and network security issues.

While not a complete coverage of security, this book has some excellent material on the subjects it covers. With limited exceptions, Stamp's writing is clear, and frequently amusing. (Unlike all too many works that try to inject humour into the security topic, Stamp's quips are

not irrelevant or distracting, but often help to address or solidify concepts.) The cryptography section is particularly good, providing items of fairly contemporary cryptological history. The references are well chosen, and a great many are available on the Web, furnishing a rich source of items for further study, or general resources. I can easily recommend this text for those interested in cryptography, and it makes some good points with regard to software security, as well.

But you can't have my copy. This one I'm keeping.

copyright Robert M. Slade, 2005 BKINSCPP.RVW 20051112
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.
niu.edu
http://victoria.tc.ca/techrev or <http://sun.soci.niu.edu/~rslade>

⚡REVIEW: "Ending Spam", Jonathan A. Zdziarski

<Rob Slade <rMslade@shaw.ca>>
Thu, 19 Jan 2006 08:16:23 -0800

BKENDSPM.RVW 20051029

"Ending Spam", Jonathan A. Zdziarski, 2005, 1-59327-052-6,
U\$39.95/C\$53.95

%A Jonathan A. Zdziarski
%C 555 De Haro Street, Suite 250, San Francisco, CA 94107
%D 2005
%G 1-59327-052-6
%I No Starch Press
%O U\$39.95/C\$53.95 415-863-9900 fax 415-863-9950 info@nostarch.

com

%O [http://www.amazon.com/exec/obidos/ASIN/1593270526/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/1593270526/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/1593270526/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/1593270526/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/1593270526/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/1593270526/robsladesin03-20)

%O Audience s+ Tech 3 Writing 2 (see revfaq.htm for explanation)

%P 287 p.

%T "Ending Spam"

The preface states that the book is for those seriously interested in spam identification technologies, and concentrates on Bayesian and related statistical filtering.

Part one is an introduction to spam filtering. Chapter one reviews the history of spam, although many of the early entries are simply annoyances or chain letters rather than the commercial or fraudulent items considered under the banner today, and the author does not seem to realize that 419 scams predated email by a considerable margin. A look at the development of spam filtering (excluding Bayesian) is presented in chapter two, along with some non-filtering. Bayesian analysis is explained in chapter three, and the statistical filtering basis is outlined in chapter four.

The fundamental actuarial core is expanded in part two. Chapter five covers message coding. Tokenization, chunking characters into identifiable items, is examined in chapter six. Tricks spammers use to evade filters, and the solutions finding spam despite the deceptions, are outlined in

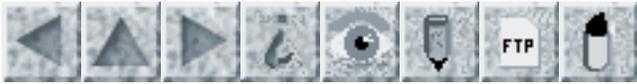
chapter

seven. Storage and performance issues raised by the data rules required by statistical filters are addressed in chapter eight. Chapter nine looks at aspects of scaling to systems supporting large numbers of users.

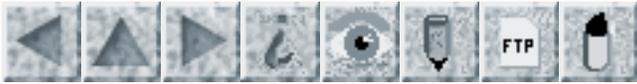
Part three deals with advanced concepts in statistical filtering. Chapter ten delves into testing which, because of the individual and adaptive nature of Bayesian filtering, presents unique challenges. Tokenization is revisited in chapter eleven, in more advanced forms. Markovian discrimination, with its examination of stateful entities, is explained in chapter twelve. Having noted many kinds of features in the book, chapter thirteen explores ways to reduce the items used (and data required) while maintaining accuracy. Collaborative rule-building with other users, groups, or systems is reviewed in chapter fourteen.

As the preface implies, this is **not** a book for users who just want to install POPFile (although that and other programs are explored in an appendix). For those who are seriously involved in managing and developing spam filtering, however, the book does provide very useful advice, pointers, and research.

copyright Robert M. Slade, 2005 BKENDSPM.RVW 20051029
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.
niu.edu
<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 17

Monday 27 February 2006

Contents

- [On learning from accidents](#)
[Don Norman](#)
- [Comparative Crash Management: OMX and TSE](#)
[Colin Brayton](#)
- [A Malfeasant Design for Lawful Interception](#)
[Diomidis Spinellis](#)
- [Active Content: Bad idea. Bad.](#)
[Rob Slade](#)
- [Even security companies get the blues](#)
[Jeremy Epstein](#)
- [Student records left exposed after computer glitch](#)
[Andrew King](#)
- [325,000 Names on Terrorism List](#)
[Daz Robert Alberti](#)
- [Behind the smoke screen of Internet and International Infrastructure](#)
[Gadi Evron](#)
- [The risks of using cell phones while driving](#)
[Nico Chart](#)

- [Some risks can be good for you, Re: redacting](#)
[Richard Karpinski](#)
 - [BOOK: Schumacher et al: Security Patterns: Integrating Security and System Engineering](#)
[PGN](#)
 - [REVIEW: "Role-Based Access Control", Ferraiolo/Kuhn/Chandramouli](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ On learning from accidents

<"Don Norman" <don@jnd.org>>
Fri, 17 Feb 2006 23:11:05 -0800

Once again we have had an accident, and once again, a well-meaning RISKSer cries out "human error" ([RISKS-24.16](#)). The airplane didn't stop in time, went off the end of the runway, collided with two cars and killed one of the car's passengers.

"Human error by the pilot, not failure of an "Automatic" system" says our faultless correspondent.

Bad pilot, says our correspondent, bad. Or, to quote the precise words,

"Perhaps in hindsight the captain honestly believes he "attempted" to deploy the Thrust-Reversers ... or maybe he's now ... trying to cover his error by an alleged system malfunction ??". I bet he feels good, our correspondent.

He has shown the world that the pilot was at fault, and now he can rest easy. No failure here -- just a bad pilot.

Sigh. You know, some 75% of accidents are blamed on human error.

Personally,
I think that figure wrong: I think those other 25% are error as well. After all, if a part failed by metal fatigue, the designer failed in not considering the possibility of fatigue. Even so-called "Acts of God" are quite predictable, at least in the statistical sense. So every failure is caused by a human somewhere along the chain. Does blaming people help us stop accidents from happening? Nope.

But, it makes people feel good to blame someone. Then they don't have think about the problem anymore, or at least not until the next time it happens. And it will, it will. Perhaps in a different form, but human error will be the culprit next time as well.

It does no good to blame something on human error. That's like saying that the communication failed because of atmospheric noise, or perhaps a component failure. What do we do when we find these physical failures? Why we devise redundant circuits, error-resistant codes, noise-tolerant communication systems. We don't blame physics and then relax. No, we do something about it.

So, why not design things so that it can tolerate the well-known forms of human error?

Case in point: the Southwest Airlines crash in Chicago, where the plane didn't manage to stop in time on a wet runway. I always want to await the final NTSB report before reaching any conclusions, but given that this has

been so badly discussed in RISKS (properly and well discussed by Peter Ladkin, I hasten to add, badly discussed by the second correspondent), let's see how we might have designed things differently.

The suspected culprit at this moment is that although the pilots computed that they had sufficient runway, the computation assumed timely deployment of the engine thrust reversers. In fact, the thrust reversers were deployed 18 seconds after touchdown. Too late -- that didn't give them sufficient time to stop the plane.

I have seen this problem before: overly precise computations produce more trust than is warranted. In one famous incident, a large cruise ship (Royal Majesty) went aground causing \$7 million of damage, to a large extent because when its GPS system failed, a dead-reckoning system took over, but still produced results accurate to two decimal places of minutes. After 30 hours of dead reckoning, the ship was 17 miles off course, but the position was still being plotted with extreme precision. Human error? Of course, although the NTSB did its usual excellent job of showing that the real culprit was the entire system, including the design of the integrated bridge navigation system.

In the Southwest Airlines incident, why did the runway-length calculator give a precise answer when the variables entered into it were so imprecise: how wet really was the runway? Just how far along the runway will the plane actually touch down? What will be its exact speed at touchdown,

its exact weight? How many seconds will it take the thrust reverser to be deployed (certainly not immediately -- 5 seconds? 10? 18?).

I propose a design rule: never give an answer with more precision than is warranted. Ideally show locations on a map as a smudge, the size comparable to the statistical likelihood. Why produce an exact stopping distance in feet? Why not produce a range, from one with everything working perfectly to one where, say, thrust reversers would not work at all, and all the other parameters were at their extreme worst ranges. Instead of displaying an exact position in hundredths of minutes or stopping distance to the foot (30 cm.), why not always show the ranges to be expected?

I don't know if this solution would have prevented this particular incident. But I do know that this philosophy can be applied to a large range of situations where today calculations are done with great precision and questionable accuracy. More importantly, the real, underlying design rule should be to learn from mistakes. To change the procedures and technology so as to mitigate against reoccurrences. Blaming the human solves no useful purpose except to make the blamer feel self-righteous. Let those who are without error cast the first blame. That would lead to zero casting.

I have tried to deliver this message many times before. I predict that I will have to give it many times again. Wouldn't it be nice if before I died, I would find it no longer necessary to deliver the message.

Don Norman, Nielsen Norman Group & Prof. EE & Computer Science,
Cognitive
Science & Psychology, Northwestern University <http://www.jnd.org>

[The RISKS archives themselves suggest that Don will have to
continue
this long-time consistent thread. PGN]

✦ Comparative Crash Management: OMX and TSE

<"Colin Brayton" <cbrayton@gmail.com>>

Mon, 20 Feb 2006 12:14:36 -0500

I have been closely following the difficulties the Tokyo Stock Exchange has been having with its trading and order management systems. As you may remember, a series of "fat finger" trades revealed that the system, which was, as it turns out, apparently in the process of being swapped out, was unable to cancel an erroneous order, causing, in the most egregious case, a \$333 million loss to the broker whose trade was input incorrectly. The software provider, Fujitsu, took the blame, and eventually a new CIO from NTT was brought in on a platform of "international best practice" for the exchange's systems.

So when the OMX, operator of a group of Scandinavian and Baltic exchanges, had what sounded like a similar problem at its Stockholm facility, I watched to see how they would handle the situation. I blogged my observations here:

<http://blogalization.nu/marketmachines/?p=3D1307> ...

The gist: All trades possibly affected by the order management fubar were automatically routed aside for manual confirmation or cancellation. The process took one hour, after which normal trading resumed.

I'm not up on the full details, but it does seem to illustrate an important point: glitches happen. What's most important is how you plan for handling them so that they don't snowball from minor glitches into loud screaming from senior government officials

Colin Brayton, Brooklyn cbrayton@gmail.com

⚡ A Malfasant Design for Lawful Interception

<Diomidis Spinellis <dds@aueb.gr>>

Sun, 19 Feb 2006 19:06:25 +0200

Earlier this month it was revealed that more than 100 mobile phone numbers belonging mostly to members of the Greek government and top-ranking civil servants were found to have been illegally tapped for a period of at least one year [1]. Apparently, the tapping was implemented by activating Ericsson's lawful interception subsystem installed at the Vodafone service provider. How could this happen?

After one looks at the design and implementation of Ericsson's Interception Management System (IMS), the real question that comes to mind is

how come such events are not happening all the time (or maybe they are?) The system is clearly not designed with security in mind.

The major problem of the design is the lack of compartmentalization. IMS is an extremely sensitive application, because it can setup and monitor the tapping of arbitrary phones. Good security engineering practice dictates that such applications should run isolated on trustworthy platforms, minimizing the surface area exposed to malicious attacks. In such a design the system's modules serve the same role as a ship's bulkheads: they provide structural stability and contain damage to specific areas.

Instead, according to its user manual [2], IMS runs on top of Ericsson's general purpose AXE exchange network management platform XMATE, which in turn runs on top of a Solaris system chock-full of support software. Among other things, XMATE provides an application programming interface, a command terminal, a macro command tool, and a file transfer application. Any of those could be conceivably exploited to activate the IMS or its functionality. In addition, the XMATE Solaris installation includes many large third party applications: the Common Desktop Environment (CDE), the Applix business performance management software [3], X.25 networking, and the OSI file transfer (FTAM). Again, security vulnerabilities in these large components could be used to seize control of the system and activate the IMS.

Even if the IMS was not installed on the network management

platform, the design of the platform apparently allows a malicious user to craft the "remote control equipment" MML commands that set up voice communication monitoring and send them to the exchange.

In a recent thought-provoking article Matt Blaze identified a number of signaling vulnerabilities in (mainly) older wiretapping systems [4].

Vulnerabilities associated with the way modern systems are designed and implemented are apparently also very important.

Disclaimer: The above is my limited understanding, based on the few documents that are publicly available. Unfortunately, documentation that would allow independent experts to assess the security of these systems is scarce. The IMS User Manual [1], although available on a number of Internet sites, is marked with red letters as "Strictly Confidential". (I guess simply "Confidential" would mean that the manual was available for download from Ericsson.) Also, the ETSI standard TR 101 943 V2.1.1 (2004-10) states in section 7.3.2: "It is also to be recommended that operational information about the LI systems, such as how they are implemented, where they reside and how they are operated and maintained, should be kept within a small group of authorized persons." Another instance where obscurity is probably used as a cover for insecurity.

[1] http://en.wikipedia.org/wiki/Greek_telephone_tapping_case_2004-2005

[2] <http://cryptome.org/ericsson-ims.htm>

[3] <http://www.applix.com/index.asp>

[4] <http://www.crypto.com/papers/wiretapping/>

Diomidis Spinellis - <http://www.dmst.aueb.gr/dds>

✶ Active Content: Bad idea. Bad.

<Rob Slade <rMslade@shaw.ca>>

Wed, 22 Feb 2006 14:04:13 -0800

Sorry, but if I've learned anything in almost 20 years of malware research, it's that active content can lead to trouble.

(And JavaScript is definitely **not** my language of choice for security purposes.)

Active cookies aim to thwart cyber crooks. A new technique to protect users against more sophisticated forms of cybercrime has been developed by Indiana University School of Informatics and affiliated start-up RavenWhite. The "active cookie" can be used as a countermeasure against online scams such as pharming and man-in-the-middle attacks. "There are no reliable commercial tools currently available to protect users from such attacks," said Jakobsson of the IU Center for Applied Cybersecurity Research. "We believe that active cookies can provide such protection." Active cookies are a "piece of cached and sandboxed executable code, such as a JavaScript object, that help authenticate an Internet browser to a server," say the researchers. The technology is a shield

against identity

theft and cyber attacks that can protect against pharming attacks as well

as techniques used to hijack Wi-Fi connections or modify consumer router

settings. Limitations include limited persistence and a lack of support

for roaming users. "And they don't offer security against strong attacks

like active corruption of routers on the client-server path, as holistic

cryptographic solutions can." Active cookies may be attractive to

financial institutions -- they complement existing techniques for user

authentication, are easy to use, and don't have the potential security

implications associated with browser plug ins.

[Source: Channel Register (UK), 21 Feb]

http://www.channelregister.co.uk/2006/02/21/active_cookie/

rslade@computercrime.org slade@victoria.tc.ca rslade@sun.soci.niu.edu

✶ Even security companies get the blues

<Jeremy Epstein <jeremy.epstein@webmethods.com>>

Fri, 24 Feb 2006 06:20:22 -0800

It was widely reported that the names, SSNs, and other personal information

for 6000 current & former McAfee employees were potentially compromised. An

auditor from Deloitte had the information on an unlabeled (but unencrypted)

CD that was left in an airplane seatback pocket. It's unknown whether the

CD simply went in the trash as part of airplane cleaning, or whether someone picked it up. McAfee is offering employees and ex-employees two years worth of credit monitoring through Experian.

The really interesting part (which I saw in the *San Jose Mercury* article, but not elsewhere) is that the auditor "had made the CD for backup purposes, and it was their decision not to encrypt the data." McAfee's spokesperson aid they have policies to prevent such actions, but they can't control what the auditor does with the data.

So if McAfee didn't have policies in place to prevent storing sensitive data in an unencrypted form (and/or to safeguard the media), Deloitte would have flunked them on their Sarbanes-Oxley audit. But because it was Deloitte who did the dirty deed, it looks like no one will be held accountable. One hopes that the Deloitte employee who made the CD is now a former employee.

Some of the news reports are commenting on the irony of it being McAfee (a security company) that lost the data; the more I think about it, the less I think that's relevant, since the fault appears to lie with Deloitte, not McAfee.

<http://www.mercurynews.com/mld/mercurynews/13950371.htm&cid=0>
http://news.com.com/Auditor+loses+McAfee+employee+data/2100-1029_3-6042544.html

P.S. I'm an ex-McAfee (actually, Network Associates) employee and did not get notified, presumably because I moved after I stopped working for them.

I've been trying to find someone at McAfee to tell me whether my information was on that CD, and if so how to get my Experian monitoring, but they make it very hard to find a contact point. If anyone has suggestions, I (and many other ex-McAfee people) would appreciate it!

[Also noted by Martyn Thomas:

<http://software.silicon.com/security/0,39024655,39156741,00.htm>

PGN]

🔴 Student records left exposed after computer glitch

<"Andrew King" <ajking@iinet.net.au>>

Mon, 20 Feb 2006 16:36:12 +0930

Thousands of [AU] Canterbury University students had their personal information exposed when online services were shut down leaving private records available to anyone with a user code and password last night.

Information such as IRD numbers, transcripts, results, outstanding payments, medical conditions, and personal addresses could all be easily accessed

online and could be changed by system users. The university's information

technology department shut down the webfront. The university had installed

a new online system late last year but there had not been any problems until

now. [Source: *New Zealand Herald*, 20 Feb 2006; PGN-ed]

[http://www.nzherald.co.nz/section/story.cfm?
c_id=1&ObjectID=10369269](http://www.nzherald.co.nz/section/story.cfm?c_id=1&ObjectID=10369269)

✦ 325,000 Names on Terrorism List (From Dave Farber's IP)

<Daz <articles.daz@gmail.com>>

Wed, 15 Feb 2006 11:25:33 -0500

Rights Groups Say Database May Include Innocent People
By Walter Pincus and Dan Eggen, *The Washington Post*, 15 Feb
2006, A01

The National Counterterrorism Center maintains a central repository of 325,000 names of international terrorism suspects or people who allegedly aid them, a number that has more than quadrupled since the fall of 2003, according to counterterrorism officials.

The list kept by the National Counterterrorism Center (NCTC) -- created in 2004 to be the primary U.S. terrorism intelligence agency -- contains a far greater number of international terrorism suspects and associated names in a single government database than has previously been disclosed. Because the same person may appear under different spellings or aliases, the true number of people is estimated to be more than 200,000, according to NCTC officials.

<...snip...>

<<http://www.washingtonpost.com/wp-dyn/content/article/2006/02/14/AR2006021402125.html?referrer=email&referrer=email>>

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

✦ 325,000 Names on Terrorism List (via Dave Farber's IP)

<Robert Alberti <alberti@sanction.net>>

Wed, 15 Feb 2006 15:28:02 -0600

"May include?" Unless Coffin vs. the United States and the Presumption of Innocence have been suspended, then the Terrorism List contains 325,000 "innocent" names.

Robert Alberti, Sanction, Inc., PO Box 583453, Mpls, MN 55458-3453
CISSP, ISSMP <http://www.sanction.net> (612) 486-5000 x211
alberti@sanction.net

✦ Behind the smoke screen of Internet and International Infrastructure

<Gadi Evron <ge@linuxbox.org>>

Sat, 18 Feb 2006 11:17:26 +0200

In the following URL for a (quick & dirty) write-up (which is too big for sending into RISKS) I start by discussing some recent threats network operators should be aware of, such as recursive DNS attacks.

Also, a bit on the state of the Internet, cooperation across different fields and how these latest threats with DDoS also relate to worms and bots, as well as spam, phishing and the immense ROI organized crime sees.

Then I try and bring some suggestions on what can be done

better, and where we as a community, as well as specifically where us, the "secret hand-shake clubs" of Internet security fail and succeed.

Over-secrecy, lack of cooperation, lack of public information, and not being secret enough about what really matters.

On the surface you can read about the attacks, how registered domains with a name created by a specific algorithm to serve as a botnet command and control server, while spammers use name servers other than their own to spamvertise from and switch back, while the DNS RR's change IP addresses every few minutes. Below the surface you will have to see what you understand as I get different responses from different people.

Looking behind the smoke screen of the Internet: DNS recursive attacks, spamvertised domains, phishing, botnet C&Cs, International Infrastructure and you

The write-up can be found here:

<http://blogs.securiteam.com/index.php/archives/298>

✶ The risks of using cell phones while driving

<"Nico Chart" <NicholasC@paradigmgeo.com>>

Thu, 16 Feb 2006 09:39:47 -0000

Here's a piece that will interest some RISKS readers: Cecil Adams ("The Straight Dope") on the risks of using cell phones while driving:

<http://www.straightdope.com/columns/060210.html>

Nico Chart, Paradigm Geophysical

[Cecil says. "Accumulating evidence suggests gabbing on the phone while driving is definitely dangerous, probably more so than other distractions."]

Some risks can be good for you, Re: redacting (Re: Jaffe, [RISKS-24.16](#))

<Richard Karpinski <dick@cfcl.com>>

Thu, 16 Feb 2006 08:22:54 -0800

> What to me seems an obvious risk was not mentioned, namely the risk of
> trusting untrusted software to perform downgrade at all, ...

This discussion would not be complete without mentioning that the more careful one wishes to be with respect to keeping something secret, the more important it may be to ensure that it is made public. The Russian success at bugging the American embassy in Moscow gave them confidence that we were NOT planning imminent hostile actions and thus kept the cold war cold somewhat more securely. Security failures in criminal and terrorist organizations are particularly valuable even in Palestine, Afghanistan, and Iraq, whether state sponsored or not. Sometimes, mistakes and inadequacies are good for us.

🔥 BOOK: Security Patterns: Integrating Security and System Engineering

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

Fri, 24 Feb 2006 9:49:32 PST

Markus Schumacher, Eduardo Fernandez-Buglioni,
Duane Hybertson, Frank Buschmann, Peter Sommerlad
Security Patterns: Integrating Security and System Engineering
John Wiley and Sons, New York, 2006
565+xxxiii

Following Christopher Alexander's inspiration, this book purports to span "the full spectrum of security in systems design", and addresses enterprise-, architectural-, and user-level security. It is the seventh book in the Wiley Series in Software Design Patterns. It includes lots of RISKS-relevant material.

🔥 REVIEW: "Role-Based Access Control", Ferraiolo/Kuhn/Chandramouli

<Rob Slade <rMslade@shaw.ca>>

Mon, 30 Jan 2006 08:01:32 -0800

BKROLBAC.RVW 20051106

"Role-Based Access Control", David F. Ferraiolo/D. Richard Kuhn/Ramaswamy Chandramouli, 2003, 1-58053-370-1

%A David F. Ferraiolo

%A D. Richard Kuhn

%A Ramaswamy Chandramouli

%C 685 Canton St., Norwood, MA 02062
%D 2003
%G 1-58053-370-1
%I Artech House/Horizon
%O 617-769-9750 800-225-9977 fax: 6177696334 artech@artech-house.com
%O <http://www.amazon.com/exec/obidos/ASIN/1580533701/robsladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/1580533701/robsladesinte-21>
%O <http://www.amazon.ca/exec/obidos/ASIN/1580533701/robsladesin03-20>
%O Audience a Tech 2 Writing 1 (see revfaq.htm for explanation)
%P 316 p.
%T "Role-Based Access Control"

The original papers on role-based access control (RBAC) saw it as an extension of mandatory access control (MAC): a given role in an organization would have a given requirement for clearance, and therefore a particular person in a role would have access to material labeled at a specific sensitivity. In the preface, the authors state that they are following current interest in RBAC as a means of identity management, with little distinction made between the use of discretionary or mandatory access control policies. The intended audiences are security professionals, software developers, and instructors and students in security courses.

Chapter one outlines the basics of access control, moves to a history of access control and RBAC, and ends with a justification for the use of RBAC in the enterprise. More details of access control concepts are provided in chapter two, along with some repetitions of the models in

chapter one. The basics of role-based access control are outlined in chapter three. Chapter four examines role hierarchies and the inheritance of privilege. Separation of duties (somewhat oversimplified in the equation to the "two man rule") addresses the issue of conflation of roles, although chapter five is rather weak in terms of practical implementation. Chapter six looks at the use of RBAC with both mandatory (MAC) and discretionary (DAC) access control. The NIST (US National Institute of Standards and Technology) RBAC standard is explained in chapter seven.

Chapter eight examines the intriguing idea of using role-based administration to manage the assignments and permissions of RBAC itself. (This material is highly formal, and would require dedicated study by those attempting to implement it.) Enterprise access frameworks (EAFs) are proposed in chapter nine, reaching back to mandatory access control for a kind of automated assignment of permissions direct from corporate policy. (Much of this text is taken up with XML code.) The relation of RBAC to various popular technologies is suggested in chapter ten. A short case study of the transition of a company to RBAC is provided in chapter eleven. Chapter twelve deals with RBAC facilities in a number of commercial products.

The writing is frequently uneven and repetitious, but the concepts are generally clear enough. The book also uses lots of acronyms, and isn't always careful about providing an explanation for them.

In regard to the stated audiences, most security professionals will find much of interest and value in the first half of the book, and it would act as a useful text in a number of security courses. Software developers might not find as much to their advantage. The second half of the book is questionable. For those involved in the formal and theoretical study of role-based access control, this work will have much merit, but that is a select audience, and the demands on the reader will be significant.

copyright Robert M. Slade, 2005 BKROLBAC.RVW 20051106
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.
niu.edu
http://victoria.tc.ca/techrev or <http://sun.soci.niu.edu/~rslade>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 18

Monday 6 March 2006

Contents

- [Cockpit usability](#)
[David Magda](#)
- [Risks of using computers in airplanes](#)
[Yvo Desmedt](#)
- [NJ Bill Would Prohibit Anonymous Posts on Forums](#)
[Lynn](#)
- [Desktop-to-mobile Malware](#)
[Peter B. Ladkin](#)
- [Re: Active content: Bad idea. Bad.](#)
[Paul Wallich](#)
- [Re: On learning from accidents](#)
[Hamish Marson](#) [Jurek Kirakowski](#) [George C. Kaplan](#)
- [New Security Paradigms Workshop: Call for Papers](#)
[John McDermott](#)
- [2006 USENIX Annual Technical Conference](#)
[Lionel Garth Jones](#)
- [REVIEW: "Practical Internet Law for Business", Kurt M. Saunders](#)
[Rob Slade](#)

● [REVIEW: "CyberRegs", Bill Zoellick](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

✈ Cockpit usability

<David Magda <dmagda@ee.ryerson.ca>>

Sun, 26 Feb 2006 12:00:10 -0500

A short-ish study [1] on the usability of aircraft avionics:

> The purpose of this study was to evaluate the accessibility of
information
> provided by the avionics system of a technically advanced
aircraft. The
> evaluation employed a tool developed by Schvaneveldt et al.
(2004) [2]
> which considers the importance of the information source when
evaluating
> information accessibility. Results showed that the TAA
avionics had
> relatively little clutter but low accessibility ratings,
especially in the
> area of Communication.

The interface showed to the operator is an important factor in
how a system
works. This topic has been discussed in RISKS on many
occasions, but I
thought this item might be of some interest.

[1] [http://psychology.wichita.edu/surl/usabilitynews/81/
AvionicsSystems.htm](http://psychology.wichita.edu/surl/usabilitynews/81/AvionicsSystems.htm)

[2] <http://www.hf.faa.gov/docs/508/docs/gaPriorityReport.pdf>

✶ Risk of using computers in airplanes

<Yvo Desmedt <y.desmedt@cs.ucl.ac.uk>>

Sat, 4 Mar 2006 11:02:15 GMT

Many years ago I told [PGN] about a Northwest Airlines airplane in Detroit unable to take off since the computer could not boot. The airline switched equipment (planes). You suggested that I should have ... sent it to RISKS.

The following item was in the **International Herald Tribune**, p. 24, in "The International Traveler Q&A", 3 Mar 2006:

... Los Angeles to London with American Airlines, we took off four hours late because of a defective computer, and then were diverted to New York to pick up a new computer ... The new computer wasn't working, so we had to change planes. We arrived in London nine hours behind schedule ...
George B. Lambrakis, London

✶ NJ Bill Would Prohibit Anonymous Posts on Forums (via IP)

<Lynn <lynn@ecgincc.com>>

Mon, 06 Mar 2006 15:22:15 -0500 (EST)

<http://yro.slashdot.org/yro/06/03/06/1736234.shtml>

NJ Bill Would Prohibit Anonymous Posts on Forums
Posted by ScuttleMonkey on Monday March 06, @02:06PM
from the glad-we're-not-in-nj dept.

Privacy The Internet

An anonymous reader writes "The New Jersey legislature is considering a bill that would require operators of public forums to collect users' legal names and addresses, and effectively disallow anonymous speech on online forums. This raises some serious issues, such as to what extent local and state governments can go in enacting and enforcing Internet legislation."

link to proposed bill:

http://www.njleg.state.nj.us/2006/Bills/A1500/1327_I1.HTM

IP Archives at: <http://www.interesting-people.org/archives/interesting-people/>

[This of course would have considerable impact on all Internet newsgroups, and opens up the question of liability that out-of-state moderators would have. It also greatly increases the difficulties for whistle-blowers who might wish to publicly air vital concerns without the obvious risks of retribution. Seems like a bad piece of legislation to me. PGN]

🔥 Desktop-to-mobile Malware

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>
Fri, 03 Mar 2006 13:19:41 +0100

An organisation called the Mobile Malware Researchers Association has said that it has identified (indeed, that it has a copy of) the

"first" virus
that can infect both Win32 desktops and Windows Mobile Pocket PC
machines
and spreads from the former to the latter.

The story was distributed by the UK IEE Newsletter this week:
[http://www.iee.org/oncomms/sector/informationpro/SectionNews/
Object/B54B7AF4-CEDB-41F9-1B0278A0A33B97E6](http://www.iee.org/oncomms/sector/informationpro/SectionNews/Object/B54B7AF4-CEDB-41F9-1B0278A0A33B97E6)

MARA can be found at <http://www.mobileav.org> along with its list
of
members.

Peter B. Ladkin, University of Bielefeld, Germany <www.rvs.uni-
bielefeld.de>

✉ **Re: Active Content: Bad idea. Bad. (Slade, [RISKS-24.17](#))**

<Paul Wallich <pw@panix.com>>
Mon, 27 Feb 2006 14:18:30 -0500

> Sorry, but if I've learned anything in almost 20 years of
malware research,
> it's that active content can lead to trouble.

This seems even worse to me than to Rob Slade. Dangerous
technology, and
deployed at (in significant part) the wrong end of the problem.
What we'd
like isn't so much to authenticate a browser (and thus,
presumably, the
person at the keyboard) to the site; what we'd like is something
to
authenticate the site to the user. At the cost of telling
legitimate users
they can only ever use one computer to get to their accounts,
the technology
does nothing about the use of stolen personal information to

establish new accounts or to establish fraudulent first-time online access to existing accounts. Meanwhile, it convinces users to set browser security in such a way that sites users believe they should trust can execute (potentially) arbitrary code. Whee.

Re: On learning from accidents (Norman, [RISKS-24.17](#))

<Hamish Marson <hamish@travellingkiwi.com>>

Tue, 28 Feb 2006 10:47:00 +0000

Back in the late 80's I was doing my degree at Massey University (NZ). In many Technology & Physics papers we were taught & graded mercilessly on getting the 'error' correct for the calculations. And showing the error on the result as well.

Everything that Don Norman says about showing the correct precision for the calculation is correct. You lost marks in exams for this. Why have we suddenly lost the ability to do it in real life now?

Could it be because much of this work is left up to young people who might be great at coding, but simply don't have an understanding of the reality behind the calculations they're being asked to program. How many people who write software actually have relevant experience in the real world for things they're doing? 10%? Probably less?

Re: On learning from accidents (Norman, [RISKS-24.17](#))

<"Kirakowski, Jurek" <jzk@ucc.ie>>

Wed, 1 Mar 2006 11:23:46 -0000

On confidence intervals around predictions:

Don Norman's well-written piece on learning from crash accidents ([RISKS-24.17](#)) highlights the major risk here but skirts around it a little, perhaps for sound, rhetorical effect. It is required engineering practice, and indeed in courts of law the same principle is applied to expert evidence: show the tolerance factor. What is the likelihood of error? How sure are you?

If you produce a prediction without assessing the confidence interval around the prediction you have just shown that you don't understand the problem you are trying to solve. If you can't answer the "likelihood of error" question in a court of law, then your status as an expert witness can be seriously undermined.

It has been said that the human race did quite well for several millions of years without statistics and confidence intervals. Well, it's time to grow up. The major RISK is that many people, even some so-called experts, fail to understand this principle.

✈ **Re: On learning from accidents (Norman, [RISKS-24.17](#))**

<"George C. Kaplan" <gckaplan@ack.berkeley.edu>>

Wed, 01 Mar 2006 11:38:41 -0800

> I have seen this problem before: overly precise computations
> produce more trust than is warranted.

I collect slide rules as a hobby. One common topic in discussions with other collectors: Modern calculators and computers make it too easy to fall into the false-precision trap (e.g. 10-digit answers to problems with 3-digit input data). It's harder to do this with a slide rule, partly because of the limited precision of the instrument, but also because the scales graphically illustrate the decreasing significance of the rightmost digits. Successively finer scale divisions are squeezed closer together, but all digits on a calculator display are equally prominent.

> I propose a design rule: never give an answer with more precision than is warranted. Ideally show locations on a map as a smudge, the size comparable to the statistical likelihood.

An excellent suggestion: Use an analog display to illustrate the limited precision that's obscured by the bare digital display.

Aviation is one of the few fields in which slide rule-type devices are still in common use, primarily as backup calculators in case the electronic systems fail. So it would be ironic if overly precise digital computations were a contributing factor in the Southwest Airlines crash.

George C. Kaplan, Communication & Network Services, University
of California
at Berkeley 1-510-643-0496 gckaplan@ack.berkeley.edu

✦ New Security Paradigms Workshop: Call for Papers

<"John McDermott (US Navy Employee)" <mcdermot@itd.nrl.navy.mil>>
Tue, 28 Feb 2006 14:50:08 -0500

NEW SECURITY PARADIGMS WORKSHOP, Call for Papers
Schloss Dagstuhl, Germany, September 18-21, 2006
Submissions due 26 March 2006
<http://www.nspw.org>

NSPW is a unique workshop that is devoted to the critical examination of new paradigms in security. Each year, since 1995, we examine proposals for new principles upon which information security can be rebuilt from the ground up. We conduct extensive, highly interactive discussions of these proposals, from which we hope both the audience and the authors emerge with a better understanding of the strengths and weaknesses of what has been discussed.

In his seminal book "The Structure of Scientific Revolutions", Thomas Kuhn describes the progress of science as "a series of peaceful interludes punctuated by intellectually violent revolutions." These revolutions, which he called "paradigm shifts", are periods during which "one conceptual world view is replaced by another."

A paradigm shift is thus not an incremental contribution to an established branch of science; it is an attempt to replace the fundamental dogma of a branch of science with a different, and completely incompatible, set of core principles.

The New Security Paradigms workshop is dedicated to the proposition that what Kuhn called "anomalies" - signs that the prevailing paradigm can no longer explain phenomena observed in the real world - are already visible in the science of information security, and, indeed, that the anomalies are so obvious and so serious that the prevailing information security paradigm is or soon will be in crisis. NSPW aspires to be the philosophical and intellectual breeding ground from which a revolution in the science of information security will emerge.

We solicit and accept papers on any topic in information security subject to the following caveats:

- 1) Papers that present a significant shift in thinking about difficult security issues are welcome.
- 2) Papers that build on a recent shift are also welcome.
- 3) Contrarian papers that dispute or call into question accepted practice or policy in security are also welcome.
- 4) We solicit papers that are not technology-centric, including those that deal with public policy issues and those that deal with the psychology and sociology of security theory and practice.
- 5) We discourage papers that represent established or completed works as well as those that substantially overlap other submitted or

published

papers.

6) We discourage papers which extend well-established security models with

incremental improvements.

7) We encourage a high level of scholarship on the part of contributors.

Authors are expected to be aware of related prior work in their topic

area, even if it predates Google. In the course of preparing an NSPW

paper, it is far better to read an original source than to cite a text

book interpretation of it.

Our program committee particularly looks for new paradigms, innovative

approaches to older problems, early thinking on new topics, and controversial issues that might not make it into other conferences but

deserve to have their try at shaking and breaking the mold.

Participation in the workshop is limited to authors of accepted papers

and conference organizers. Each paper is typically the focus of 45

to 60 minutes of presentation and discussion. Prospective authors are

encouraged to submit ideas that might be considered risky in some other

forum, and all participants are charged with providing feedback in a

constructive manner. The resulting intensive brainstorming has proved to

be an excellent medium for furthering the development of these ideas. The

proceedings, which are published after the workshop, have consistently

benefited from the inclusion of workshop feedback.

We welcome three categories of submission:

1) Research papers. These should be of a length commensurate

with the

novelty of the paradigm and the amount of novel material that the

reviewer must assimilate in order to evaluate it.

2) Position papers. These should be 5 - 10 pages in length and should

espouse a well reasoned and carefully documented position on a security

related topic that merits challenge and / or discussion.

3) Discussion topic proposals. Discussion topic proposals should include an

in-depth description of the topic to be discussed, a convincing argument

that the topic will lead to a lively discussion, and supporting materials

that can aid in the evaluation of the proposal. The later may include

the credentials of the proposed discussants. Discussion topic proposers

may want to consider involving conference organizers or previous

attendees in their proposals.

Submissions must include the following:

1) The submission in PDF format, viewable by Adobe Acrobat reader.

2) A justification for inclusion in NSPW. Specify the category of your

submission and describe, in one page or less, why your submission is

appropriate for the New Security Paradigms Workshop. A good justification

will describe the new paradigm being proposed, explain how it departs

from existing theory or practice, and identify those aspects of the

status quo it challenges or rejects. The justification is a major factor

in determining acceptance.

3) An Attendance Statement specifying how many authors wish to attend the workshop. Accepted papers require the attendance of at least one author for the entire duration of the workshop. Attendance is limited, and we cannot guarantee space for more than one author.

No submission may have been published elsewhere nor may a similar submission be under consideration for publication or presentation in any other forum during the NSPW review process.

The submission deadline is Monday, 26 March 2006.
Notification of acceptance will be Monday, 28 May, 2006.

See <http://www.nspw.org> for details of the workshop policies and for submission procedures.

John McDermott, Publicity Chair, New Security Paradigms Workshop '06

[Slightly pruned for RISKS. This is a very important workshop. PGN]

2006 USENIX Annual Technical Conference

<Lionel Garth Jones <lgj@usenix.org>>
Mon, 06 Mar 2006 14:37:05 -0800

2006 USENIX Annual Technical Conference
May 30-June 3, 2006, Boston, MA
<http://www.usenix.org/usenix06/proga>
Early Bird Registration Deadline: May 12, 2006

We're pleased to invite you to attend the 2006 USENIX Annual

Technical

Conference. This year we're offering 5 days of training running alongside a 3-day conference program filled with the latest research, security breakthroughs, and practical approaches to the questions and problems you wrestle with. You'll also have many opportunities to chat with peers who share your concerns and interests.

--- Training: Tuesday-Saturday, May 30-June 3, 2006

USENIX '06 offers 5 days of tutorials led by highly respected Instructors covering crucial topics including:

- * Measuring Security, Dan Geer
- * Ajax and Advanced Responsive WebApp Development, Alex Russell
- * Administering Linux in Production Environments, AEleen Frisch
- * Building a Logging Infrastructure and Log Analysis for Security, Abe Singer
- * Defense Against the Dark Arts: Repelling the Wily Hacker, Bill Cheswick

To view the entire training program, see:

<http://www.usenix.org/events/usenix06/training/>

--- Technical Sessions: Thursday-Saturday, June 1-3, 2006

The 3-day technical program begins with the keynote address:

"Planetlab:

Evolution vs. Intelligent Design in Planetary-Scale Infrastructure," by

Larry Peterson, Princeton University and PlanetLab Consortium, and includes

other Invited Talks of note, such as:

* Plenary Session: "Why Mr. Incredible and Buzz Lightyear Need Better Tools:

Pixar and Software Development," by Greg Brandeau, Vice President of

Technology, Pixar Animation Studios

* Closing Session: "Real Operating Systems for Real-time Motion Control," by

Trevor Blackwell, CTO, Anybots

* Peiter "Mudge" Zatko, BBN Technologies, on "Success, Failure, and Alternative Solutions for Network Security"

* Matt Welsh, Harvard University, on "Deploying a Sensor Network on an Active Volcano"

* And more!

The Systems Practice and Experience track is the premier forum for presenting the latest in groundbreaking research. Be among the first to check out the latest innovative work on the topics you need most. Check out the full technical program at:

<http://www.usenix.org/events/usenix06/tech/>

Finally, don't miss the opportunity to pose your toughest questions to the experts in the Guru Is In Sessions. Mingle with colleagues and leading experts at the Birds-of-a-Feather sessions and at the various evening social events, including a Poster Session & Happy Hour, vendor sessions, and an off-site conference reception.

USENIX '06 promises to be an exciting showcase for the latest in innovative research and cutting-edge practices in technology. We look forward to seeing you in Boston in May. Register today at:

<http://www.usenix.org/events/usenix06/registration/>

On behalf of the USENIX '06 Organizers,

Atul Adya, Microsoft

Erich Nahum, IBM T.J. Watson Research Center
USENIX '06 Program Co-Chairs

2006 USENIX Annual Technical Conference
May 30-June 3, 2006, Boston, MA

<http://www.usenix.org/usenix06/proga>

Early Bird Registration Deadline: May 12, 2006

REVIEW: "Practical Internet Law for Business", Kurt M. Saunders

<Rob Slade <rMslade@shaw.ca>>

Mon, 13 Feb 2006 08:01:36 -0800

BKPRILFB.RVW 20051117

"Practical Internet Law for Business", Kurt M. Saunders, 2001,
1-58053-003-6, U\$73.00

%A Kurt M. Saunders

%C 685 Canton St., Norwood, MA 02062

%D 2001

%G 1-58053-003-6

%I Artech House/Horizon

%O U\$73.00 800-225-9977 fax: 617-769-6334 artech@artech-house.
com

%O [http://www.amazon.com/exec/obidos/ASIN/1580530036/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/1580530036/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/1580530036/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/1580530036/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/1580530036/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/1580530036/robsladesin03-20)

%O Audience s- Tech 1 Writing 2 (see revfaq.htm for
explanation)

%P 162 p.

%T "Practical Internet Law for Business"

The preface states that this book is intended to allow business
and
system managers to understand the legal issues surrounding

electronic
commerce.

Chapter one provides a brief and basic historical overview of the Internet, stressing the decentralized nature, and the fact that nobody is in charge. Jurisdiction, and the rulings in regard to it, are discussed in chapter two. (Somewhat ironically, in view of the topic, while international decisions are mentioned, the material is definitely oriented to the legal system of the United States.) Encryption is the topic of chapter three, which deals with export controls on cryptographic software (even though the regulations have been extensively liberalized) and electronic signature laws (even though many of these laws allow for completely unencrypted "signatures"). Chapter four very briefly examines the issue of trade secrets, seemingly without much relation to the Internet. Trademarks, on the other hand, do have a great deal of relevance to the net in cybersquatting cases and the like, and are addressed in chapter five. Some of the material on copyright, in chapter six, repeats content dealt with in chapter five. Chapter seven provides an interesting and detailed examination of email privacy in the workplace. Chapter eight is rather vague, since its definition of "online crime" is not very specific. (Some of the case law presented is also reported simplistically: the account of United States vs Thomas, for example, does not deal with the issue of community standards that made the material legal in California but not in Tennessee.) The book closes with patent law, in chapter nine (oddly separated from the other intellectual property topics in chapters four to six), most of which deals with the non-patentability of software.

This work is a lot about law, and not very much about the Internet.

How practical it may be is a question that individual readers will have to answer.

copyright Robert M. Slade, 2005 BKPRILFB.RVW 20051117
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.
niu.edu
http://victoria.tc.ca/techrev or <http://sun.soci.niu.edu/~rslade>

REVIEW: "CyberRegs", Bill Zoellick

<Rob Slade <rMslade@shaw.ca>>
Mon, 06 Mar 2006 11:14:05 -0800

BKCBRRGS.RVW 20051202

"CyberRegs", Bill Zoellick, 2002, 0-201-72230-5, U\$39.99/C\$59.95

%A Bill Zoellick

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8

%D 2002

%G 0-201-72230-5

%I Addison-Wesley Publishing Co.

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

%O <http://www.amazon.com/exec/obidos/ASIN/0201722305/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/0201722305/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/0201722305/robsladesin03-20>

%O Audience i Tech 1 Writing 2 (see revfaq.htm for explanation)

%P 307

%T "CyberRegs: A Business Guide to Web Property Privacy and Patents"

The introduction states that the nature of the Web is in flux. Those who take too strong and doctrinaire a stance on the character of the Internet will be subject to failures in their attempts to do business there. In addition, the author states his opinion, based on the research conducted for the book, that attempts to apply regulation to the net should be sparing.

Part one deals with copyright. Chapter one reviews the past history of copyright legislation and purposes, and also the recent case of Napster. (The book was completed before the Napster case concluded.) "DVD Jon" and the DeCSS case is the topic of chapter two. The author's experiences with the publishing and sale of special reports forms the basis for an examination of licensing, in chapter three, and also the balance of rights between publisher and user/consumer. The development and shift in copyright regulations and perspectives is given in chapter four. Chapter five lists further reading on the topic: an annotated bibliography of text and online sources. The works are well chosen and the annotations provide good overviews of the material.

Part two addresses patents. Chapter six outlines the Amazon "1-Click" patent, and the issue of an idea versus a specific implementation. A variety of other patents and lawsuits are examined in chapter seven. Chapter eight deals with the issue of patentability of an entity or item. The issue of patenting business methods is dealt with in chapter nine.

Chapter ten examines the impact of patents on the Internet. Walker Digital and the business of creating and holding business patents is in chapter eleven. Recent US legislation amending patent concepts and applicability is covered in chapter twelve. Chapter thirteen opines about the future and fourteen closes off the topic with the reference section.

Part four surveys electronic signatures and the E-Sign act. Chapter fifteen discusses the provisions of the act itself, including the fact that it doesn't (in any significant way) define what an electronic signature can be, thus obviating the need for many of the functions of a signature. (This is followed by a brief section entitled "A Deeper Look" that explains the technical concept of digital signatures.) Business will increase because of the act, says chapter sixteen. Chapter seventeen makes the case (rather weakly, perhaps) that E-Sign is a good act, because it doesn't impede allowable technologies. Eighteen is the references chapter for electronic signatures.

Part four moves in on privacy. Chapter nineteen cites a couple of cases of the market for private information. US legal precedents regarding the right to privacy are in chapter twenty. Consumer concerns, in chapter twenty-one, are followed up by "A Deeper Look" at cookies and Web bugs, and by another on the Platform for Privacy Preferences Project (P3P). US legislative moves regarding privacy are discussed in chapter twenty-two. (It is interesting to note that Zoellick quotes a legislator stating that privacy

acts would be passed before 2002. This did not happen. In addition, of the various aspects discussed in the chapter, bill S.1789, before the Senate as this review is being written, addresses only access and enforcement.) Chapter twenty-three tries, without much success, to propose a framework for privacy. Again, twenty-four contains references.

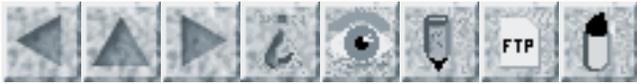
An epilogue finishes out the book by opining that businesses can, and should, work at understanding the Web better, so that they can shape its future development. As long as they develop it the way the author suggests.

Oddly, this work does not seem to add materially to other discussions of Internet law. That it examines intellectual property issues in such depth is interesting, but not illuminating. However, Zoellick does have a much more engaging writing style than other authors who have written on legal topics in relation to the net, and the text is much more readable than most such books. There is a good deal of valuable information in this volume on the subjects examined: but there is a lot of opinion as well.

copyright Robert M. Slade, 2005 BKCBRRGS.RVW 20051202
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.
niu.edu
http://victoria.tc.ca/techrev or [http://sun.soci.niu.edu/
~rslade](http://sun.soci.niu.edu/~rslade)



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 19

Friday 10 March 2006

Contents

- [Technical Problems Cause Errors in SAT Test Scores](#)
[Karen W. Arenson via PGN](#)
- [Officials Say Scoring Errors for SAT Were Understated](#)
[Karen W. Arenson via Monty Solomon](#)
- [Watered-Down SAT Scores!](#)
[Chuck Weinstock](#)
- [Complexity causes 50% of product returns](#)
[PGN](#)
- [Onboard Emissions Chip Major Malfunction](#)
[Colin Brayton](#)
- [Excel garbles microarray experiment data](#)
[Mark Liberman](#)
- [Citibank Blocks Some Debit-Card Use Abroad](#)
[Monty Solomon](#)
- [Government surplus sale yields personal data](#)
[Karl Klashinsky](#)
- [Australian National Credit Union Limits Internet Passwords](#)
[evant](#)

- [More stupid high-tech legislation in NJ](#)
[Walter Dnes](#) [Tanner Andrews](#) [Rex Black](#)
 - [Re: On learning from accidents](#)
[Martyn Thomas](#) [Jerome Ravetz](#) [Perry Bowker](#) [Richard Karpinski](#)
 - [Insecure APC BioPod](#)
[Gabe Goldberg](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ "Technical Problems Cause Errors in SAT Test Scores"

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

Wed, 8 Mar 2006 15:30:27 PST

On the order of 4000 students taking the October 2005 Scholastic Aptitude Tests (SATs) received scores lower than they should have been, due to unexplained "technical problems". Some scores on the reasoning section were as much as 100 points too low (out of 800). This may be unfortunate for those students, considering that the final acceptances and rejections are being decided before the affected universities have been notified. Similar scanning problems were noted in an earlier SAT chemistry test, although on a smaller scale. [Source: Karen W. Arenson, *The New York Times*, 8 Mar 2006, National Edition A16; PGN-ed]
<http://www.nytimes.com/2006/03/08/education/08sat.html>

⚡ Officials Say Scoring Errors for SAT Were Understated

<Monty Solomon <monty@roscom.com>>

Thu, 9 Mar 2006 10:17:18 -0500

A day after the College Board notified colleges that it had misreported the scores of 4,000 students who took the SAT exam in October, an official of the testing organization disclosed that some of the errors were far larger than initially suggested. ... Chiara Coletti, the College Board's vice president for public affairs, said that 16 students out of the 495,000 who took the October exam had scores that should have been more than 200 points higher. "There were no changes at all that were more than 400 points."

[Source: Karen W. Arenson, *The New York Times*, 9 Mar 2006]

<http://www.nytimes.com/2006/03/09/education/09sat.html?ex=1299560400&en=ada0b50e98bcfb5f&ei=5090>

Watered-Down SAT Scores!

<Chuck Weinstock <weinstock@sei.cmu.edu>>

Fri, 10 Mar 2006 09:12:11 -0500

Pearson Educational Measurement suggests that wet weather may have caused the 4000 affected test results, blaming abnormally high moisture for expanding the paper so that it could not be read properly at a scanning center in Austin TX. The test on 8 Oct 2005 coincided with the beginning of heavy rains in the Northeast, from where most of those tests came. (As much as 10 inches fell on New Jersey.) [Source: AP item on 10 Mar 2006.]

✦ Complexity causes 50% of product returns

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

Thu, 9 Mar 2006 14:23:39 PST

Perhaps relevant to Don Norman's research on human interfaces, Elke den

Ouden's thesis at the Technical University of Eindhoven concluded that half

of all supposedly malfunctioning products returned to stores were in reality

in full working order, but just too complex to be operated successfully.

She also noted that the average U.S. consumer will spend a maximum of about

20 minutes trying to get a newly acquired electronics device to work before

giving up.

<http://abcnews.go.com/Technology/wireStory?id=1693288>

✦ Onboard Emissions Chip Major Malfunction

<"Colin Brayton" <cbrayton@gmail.com>>

Wed, 8 Mar 2006 15:21:05 -0500

Drivers in Missouri discovered that the onboard chips that monitored their

auto emissions could fail, causing certification failure, and could then

then be an unbelievable bother to reset:

Alter got a "drive cycle," or a step-by-step recipe to reset the car's

computer by driving 10 minutes or more at 50 to 65 mph, then coasting down to 15 mph without hitting the brakes until the car reaches 20 mph. Then he had to stop and let the car idle for 50 seconds or more before taking the car back up to highway speeds, then gradually slowing until the car came to a stop.

Nothing. The car still was rejected. Nine times in all.

"It was like, well, what do I do now?" he said. "I am driving around, doing this, putting (a couple hundred) miles on it. So is it inconvenient? Yeah.

A big inconvenience. The amount of gas I wasted. And my time."

Finally, he discovered a shop whose repair technician drove his car while monitoring its readiness codes with a mobile computer. Once the codes reset, the technician took the car for a test.

The cost: \$120 for two hours of the technician's time. Illinois test officials say they see the problem in about 1 percent to 2 percent of all on-board diagnostic tests.

Sources: *St. Louis Dispatch*, 25 Feb 2006

<<http://www.stltoday.com/stltoday/news/stories.nsf/stlouiscitycount=y/story/C1B49084DF769D42862571200022E77F?OpenDocument>>

New Market Machines <<http://blogalization.nu/marketmachines/?p=3D1495>>(my blog)

Excel garbles microarray experiment data

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

Fri, 10 Mar 2006 8:31:32 PST

[TNX to Fernando Pereira for putting me on to this one.]

<http://itre.cis.upenn.edu/~myl/languagelog/>

<http://itre.cis.upenn.edu/~myl/languagelog/archives/002912.html>

The December 1 DWIM effect [The Cupertino effect, 9 Mar 09, 2006]

The damage done by well-intentioned (mis)features of MS Office is not

limited to occasional dadafication of EU bureaucratese

<<http://itre.cis.upenn.edu/%7Emyl/languagelog/archives/002911.html>>.

According to Barry R Zeeberg, Joseph Riss, David W Kane, Kimberly J Bussey,

Edward Uchio, W Marston Linehan, J Carl Barrett and John N Weinstein,

"Mistaken Identifiers: Gene name errors can be introduced inadvertently when

using Excel in bioinformatics

<<http://www.biomedcentral.com/1471-2105/5/80>>", BMC

Bioinformatics 2004,

5:80:

When we were beta-testing [two new bioinformatics programs] on microarray

data, a frustrating problem occurred repeatedly: Some gene names kept

bouncing back as "unknown." A little detective work revealed the reason:

... A default date conversion feature in Excel ... was altering gene names

that it considered to look like dates. For example, the tumor suppressor

DEC1 [Deleted in Esophageal Cancer 1] was being converted to '1-DEC.'

Figure 1 lists 30 gene names that suffer an analogous fate.

A worse problem apparently afflicts information from microarray

experiments:

There is another default conversion problem for RIKEN clone identifiers

identifiers of the form nnnnnnnnEnn, where n denotes a digit. These

identifiers are comprised of the serial number of the plate that contains

the library, information on plate status, and the address of the clone. A

search ... identified more than 2,000 such identifiers out of a total set

of 60,770. For example, the RIKEN identifier "2310009E13" was converted

irreversibly to the floating-point number "2.31E+13." A non-expert user

might well fail to notice that approximately 3% of the identifiers on a

microarray with tens of thousands of genes had been converted to an

incorrect form, yet the potential for 2,000 identifiers to be transmogrified without notice is a considerable concern. Most important,

these conversions to an internal date representation or floating-point

number format are irreversible; the original gene name cannot be

recovered.

RIKEN <<http://www.jarvislab.net/Genomics.html>> microarrays are systematically affected, but other microarray results are apparently often garbled as well:

The floating-point conversion is not restricted to RIKEN clone identifiers

but will affect any clone designation derived from plate coordinates. ... [If plate library references are omitted or numerical],

all clones from row E of any plate are converted to floating point numbers

by Excel. ... Since 96-well plates contain 8 rows and 12 columns, row E

represents 12/96 or 12.5% of the clones on the plate;
similarly, 6.25% of
clones from 384-well plates would be affected. Most libraries
contain
hundreds of plates, each of which would be subject to this
problem.

If some computer virus or trojan did this sort of damage to the
results
of thousands of high-cost biomedical experiments, I imagine that
we'd
see a serious effort to put some people in jail. I'm not
suggesting that
any similar sort of retribution is appropriate here, but perhaps
some
rehabilitation would be in order, along the lines suggested
below.

There's an acronym from the old days of classic AI, DWIM,
standing for
"Do What I Mean". The Jargon File explains
<<http://www.catb.org/%7Eesr/jargon/html/D/DWIM.html>>:

Warren Teitelman originally wrote DWIM to fix his typos and
spelling
errors, so it was somewhat idiosyncratic to his style, and
would often
make hash of anyone else's typos if they were stylistically
different. Some victims of DWIM thus claimed that the acronym
stood for
"Damn Warren's Infernal Machine!".

In one notorious incident, Warren added a DWIM feature to the
command
interpreter used at Xerox PARC. One day another hacker there
typed delete
*\$ to free up some disk space. (The editor there named backup
files by
appending \$ to the original file name, so he was trying to
delete any
backup files left over from old editing sessions.) It happened
that there
weren't any editor backup files, so DWIM helpfully reported *\$

not found,

assuming you meant 'delete *'. It then started to delete all the files on

the disk! The hacker managed to stop it with a Vulcan nerve pinch after

only a half dozen or so files were lost.

The disgruntled victim later said he had been sorely tempted to go to

Warren's office, tie Warren down in his chair in front of his workstation,

and then type delete *\$ twice. DWIM is often suggested in jest as a

desired feature for a complex program; it is also occasionally described

as the single instruction the ideal computer would have. Back when proofs

of program correctness were in vogue, there were also jokes about DWIMC

(Do What I Mean, Correctly).

It seems to me that all interactive programs should have a prominently

displayed switch labeled something like DEWITYD, "Do Exactly What I Tell

You, Damnit!" (pronounced as "de-witted"). No doubt the results will be

wrong (or even disastrous) at least as often as the results of DWIM will be;

but at least you'll know exactly who to blame.

Posted by Mark Liberman at March 9, 2006 05:51 PM

<<http://www.sitemeter.com/stats.asp?site=sm7languageblog>>

[I always enjoyed seeing Warren's license plate (DWIM) now and then while

driving. However, based on experience with InterLisp, many wags suggested

that the correct acronym should have been DWWTYM -- Do What Warren Thinks

You Mean. PGN]

✶ Citibank Blocks Some Debit-Card Use Abroad

<Monty Solomon <monty@roscom.com>>

Wed, 8 Mar 2006 12:40:13 -0500

Citibank said has blocked the use of some of its PIN-based debit cards after detecting fraudulent cash withdrawals in Britain, Canada and Russia. PINs were apparently obtained from "a third-party business' information breach" in the U.S. last year. [Source: Eileen Alt Powell, AP Online, 8 Mar 2006; PGN-ed]

<http://finance.lycos.com/home/news/story.asp?story=56481434>

[Apparently the PINs are archived, perhaps even unencrypted? PGN]

<http://www.msnbc.msn.com/id/11731365/>

✶ Government surplus sale yields personal data

<Karl Klashinsky <klash@cisco.com>>

Tue, 07 Mar 2006 11:03:09 -0800

Health and immigration records sold at B.C. auction
(news item from the Canadian Broadcasting Corp)

Several investigations have begun after computer tapes containing health and immigration records for thousands of people in British Columbia were sold at a public auction for \$101.

<http://www.cbc.ca/story/canada/national/2006/03/06/bc-government->

[tapes060306.html](#)

The records contained information on sexual abuse, HIV status, and mental health, as well as other information that was obviously quite confidential in nature.

The fact that old backup tapes were sold off is probably not too surprising to RISKS readers. What is interesting is that this is not the first time, and, according to the article, "the government brought in rules that should have ensured that all information was removed from surplus computer equipment before it was sold."

⚡ Australian National Credit Union Limits Internet Passwords

<evant@netspace.net.au>

Wed, 8 Mar 2006 16:00:16 +1100

A step backwards for customers of Australian National Credit Union (www.friendlybanking.com.au) where from 21 Mar 2006 all users of the credit union's Internet banking will be limited to choosing passwords of six characters, consisting only of the numbers 0-9. They have previously had the ability to choose alpha-numeric passwords of varying length.

The credit union's website claims that the changes are for enhanced security

(http://www.friendlybanking.com.au/Pages/view_news.asp?news_id=1999):

Important Internet Banking Password Changes

As of 21st March 2006, passwords for Internet Banking will be changing. This will apply to all passwords and second passwords (where applicable). Your Internet Banking password will now be known as your Web Access Code (WAC).

Web Access Codes (WAC) must now be six (6) digits long and only contain numbers (0 - 9), but no spaces. Make sure it is difficult for others to guess and does not contain your date of birth, member number and repeated digits.

Please do not change your WAC until you are prompted to on or after the 21st March 2006. This will save you having to re enter a new WAC.

These changes are being made in preparation for an improved site later in the year with added functionality such as Bpay view, Secure mail, Setting up regular payments, Submit a request for a new Term Deposit, Added security features.

After I enquired about this apparent backward step, the credit union's response claimed this was required for the implementation of two-factor authentication, amongst other security enhancements. Two-factor authentication might be great for those who use it, but those that don't will be left with the limited password options.

I thought the RISKS were obvious, but perhaps not to the credit union's security team.

⚡ **More stupid high-tech legislation in NJ ([RISKS-24.19](#))**

<"Walter Dnes" <waltdnes@waltdnes.org>>

Tue, 7 Mar 2006 23:38:35 -0500

High-tech-howlers are nothing new for New Jersey legislators.
See

<http://catless.ncl.ac.uk/Risks/12.09.html#subj5> back in 1991.

That was

about a bill that would require all "software engineers" to be
licenced, for

a **VERY WIDE** definition of "software engineer". The initial
draft would've

required every secretary who created a Word or Excel macro to be
licenced as
an engineer.

Walter Dnes <waltdnes@waltdnes.org> In linux /sbin/init is Job #1

⚡ **Re: NJ Bill Would Prohibit Anonymous Posts on Forums ([RISKS-24.19](#))**

<tanner andrews <tanner@payer.org>>

Mon, 6 Mar 2006 23:03:08 -0500 (EST)

Too much important opinion, including that leading to the
founding of the
country, was published anonymously to permit the government to
ban anonymous
opinion. Even unto this day, anonymous pamphleteering is an
honorable
activity at the core of the First Amendment.

The main difference between Mrs. McIntyre's pamphlets and the

fora to be regulated is that a reader could use the pamphlet to create litter. The Internet provides no similar opportunity because one is not handed an physical object.

I would expect that such a statute, were it to be enacted, would be quickly challenged and almost as quickly overturned. See *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995). Nor is the question of littering dispositive. See *Schneider v. NJ*, 308 U.S. 147 (1939) [156, Milwaukee; 157, Worcester].

Obviously I am not a lawyer and you would talk to one before challenging or violating any statute.

Re: NJ Bill Would Prohibit Anonymous Posts on Forums ([RISKS-24.18](#))

<Rex Black <rexblack@ix.netcom.com>>

Mon, 06 Mar 2006 22:45:37 -0600

On the other hand, having had a few "hit job" reviews posted of my book, **Managing the Testing Process**, posted at Amazon.com by anonymous reviewers, it seems that allowing people to slam other people--who may well be competitor's--in a public forum without disclosing their identities and therefore their interests poses some risks not just to the people who are slammed, but also to the readers who may unquestioning accept

the critique
while unaware of the motivations and interests behind the
critique.

Rex Black, CTO, Pure Testing, Pvt Ltd; President, American
Software Testing
Qualifications Board; President, International Software Testing
Qualifications Board; 31520 Beck Road, Bulverde, TX 78163 +1
(830) 438-4830
www.rexblackconsulting.com

Re: On learning from accidents (Kirakowski, [RISKS-24.18](#))

<"Martyn Thomas" <martyn@thomas-associates.co.uk>>
Tue, 7 Mar 2006 09:48:48 -0000

When was the last time you saw a safety case where the claimed
probabilities
of failure had error bounds?

When was the last time you saw a sound argument justifying these
error
bounds? I never have.

Has anyone on the list **written** such a safety case?

Re: On learning from accidents (Norman, [RISKS-24.17](#))

<Jerome Ravetz <jerome-ravetz@tiscali.co.uk>>
Tue, 7 Mar 2006 14:07:05 +0000

Up to now the most obvious harm done by pseudo-precision may
well be in the
'accidents' of badly designed systems. It could also be that

the failure to control the mass of meaningless output from computer programs ('GIGO science') is a consequence of our dogmatic faith in numbers. My education in pseudo-precision began when I realised that students being taught the Systeme Internationale as promoted in England in 1970 were forced to lie. At that time, the S.I. prefixes were rigorously cascaded in thousands; the deci- and centi- were banned. So students doing exercises in 'the metric system' were required to quote measurements of length to the nearest millimetre, even when the object was a rough concrete pillar. Like Hamish Marson I knew some old-fashioned physical scientists who taught their students about the management of uncertainty; but the breed was dying out even then.

Reflecting on all this I eventually wrote (with my colleague Silvio Funtowicz) 'Uncertainty and Quality in Science for Policy'. In this we developed the 'NUSAP' notational scheme, whose categories are Numeral, Unit, Spread, Assessment and Pedigree. The principle behind NUSAP has had some success; the Dutch Environment Agency has a 'Guidance' for assessing uncertainty in scientific information which is becoming a standard. But even there I find inadequate attention to the task of matching precision to accuracy. And for the situations when very uncertain quantities are involved (as in much policy-related information) I find hardly any concern at all.

Are there RISKS readers interested in developing this?

Jerry Ravetz, 111 Victoria Road, Oxford OX2 7QG, +44 [0]1865 512247

Mobile 0790 535 2788 Website: www.jerryravetz.co.uk
Visiting Fellow, the James Martin Institute for Science and Civilization, Business School, Oxford University.

Files of my recent papers, available for downloading, can be found on the website www.nusap.net; on the Home Page see Tutorials - Post-Normal Science and NUSAP, and Sections - Reports, papers.

✶ Re: On learning from accidents (Norman, [RISKS-24.17](#))

<Perry Bowker <pbowker@sympatico.ca>>

Thu, 09 Mar 2006 10:27:35 -0500

The discussion of error tolerances reminded me of a time, many years ago, when I was an undergrad physics student. We were, of course, drilled endlessly by professors and post-grad assistants about the vital need to include error bars in experimental results. One day, my lab partner and I were running some experiment (I think it was to explore a Wheatstone bridge) built out of ancient wires, resistances, and meters. The hopelessly antique equipment inspired my partner to record some result as "4.1487892 +/- .002%" in his lab book. When the experiment was marked, the instructor wrote "I don't see how you could have achieved such precision", to which my partner wittily wrote back: "You should not be critical of extra work,

voluntarily
done."

⚡ **Re: On learning from accidents (Marson, [RISKS-24.18](#))**

<<dick@cfcl.com>>

Mon, 6 Mar 2006 21:16:46 -0800

Relevant experience? (gotta understand)

Hamish Marson asks, How many people who write software actually have relevant experience in the real world for things they're doing?

In my view, relevant experience is not near enough to do the job right.

Usually when a task is to be done using a computer, the designers and coders must understand the task BETTER than most real world experts do. Otherwise it doesn't work and nobody is happy. Furthermore, there are many other ways to fail, as well. Some of them are profitable anyway.

⚡ **Insecure APC BioPod**

<Gabe Goldberg <gabe@gabegold.com>>

Wed, 08 Mar 2006 22:06:21 -0500

APC (American Power Conversion) <http://apc.com/> sells a BioPod <http://apc.com/products/family/index.cfm?id=246&ISOCountryCode=ww> described "Biometric Security: A Simple and Secure Way to Remember Passwords".

Text is "As security concerns continue to grow, so do the number of passwords. The Biometric Password Manager provide users a convenient and secure way to manage and access multiple security phrases and codes. This product biometrically identifies users and gives them convenient access to password protected applications and web sites."

When you install the software, it uses your Windows password for securing all your login/password pairs. That's of course bad because you might want more or layered security on your logins. What's worse is that if you have no Windows password the software silently accepts null as password. That is, not only do you not need a password to open the password vault stored on the BioPod, no warning is given that a password might be a good idea to secure the goodies.

After getting over my astonishment at that behavior I called APC tech support but couldn't convince them that there was a problem. The dialogue below shows my repeated failed attempts to convince the Web folk that a problem exists.

=====

Me: Biopod has huge security flaw, compromises the device's integrity.

I've reported this to your support people but see no action taken.

APC: Thank you for contacting APC's email support on 01/31/2006 06:27

PM. I would be happy to assist you.

I apologize for the inconvenience. I am unaware of any security flaw with the BioPod. If you would like to describe the details of the suspected please feel free to send them to me. Officially the BioPod is not advertised as a security device, but a password manager, so it is not designed to increase the security of your computer, but provide a safe way to manage and store your passwords.

Me: Installing the BioPod software on a Windows PC that is not password protected makes the BioPod password blanks. That is, when the password challenge is issued simply clicking OK without using a fingerprint AND WITHOUT ENTERING A PASSWORD logs in to the BioPod password vault.

That's not my idea of a useful password manager.

APC: The OmniPass software and BioPod can be setup for use with a Windows password or without a Windows password. If you don't have a Windows password and setup a "Windows" user you will be able to log into the password vault without a password because you don't have a Windows password. If you don't want to setup a Windows password simply setup a non-Windows user in OmniPass by following the directions in the attached document.

Me: You're entirely missing my point. NO WARNING IS GIVEN THAT THE BIOPOD HAS BEEN SET UP WITH NO PASSWORD. THIS IS A PROFOUND SECURITY EXPOSURE SINCE IT GIVES THE ILLUSION OF PROTECTION WHERE THERE IS

NONE. Do you think the BioPod is performing correctly and that it's documented correctly and fully? If so, we have nothing further to discuss -- but I'm astonished at APC's (lack of) response to this problem.

APC: I understand your point, however if you choose to setup a BioPod user using your Windows password as the master password and your Windows

Password is blank, the BioPod would clearly not have a secure Master

Password. It is for this reason if you do not have a Windows password it

is recommended you use choose the option to setup a separate Master

Password not based on the Windows password. Or you could opt to add

security to your computer system by adding a Windows password.

Me: This is your last chance. I reinstalled the software to review the

installation dialogue. If no Windows password is set NO WARNING IS GIVEN

THAT THE DEVICE IS NOT SECURE. You're correct that the user can set a

Windows password for the specific purpose of having it inherited by the

BioPod, and then remove the Windows password. But doesn't this seem a bit

cumbersome to you? And aren't users unlikely to do it WITHOUT SPECIFIC

INSTRUCTIONS?

Having the BioPod only take the Windows password, being unable to set a

specific unique password for the BioPod, is very bad design. Your

unwillingness to acknowledge that users MAY NOT REALIZE THAT THEIR BIOPOD

is insecure is baffling.

So my next communication will be with your public relations people and some mailing lists that publicize security risks such as this. They'll of course see how many times I tried to convince you that there's a problem here.

APC: When the BioPod and OmniPass software are used properly they provide a secure way to manage your passwords. For more information about the operation of the software please contact Softex Inc, the designer of the software at www.softexinc.com support@softexinc.com.

Gabriel Goldberg, Computers and Publishing, Inc., 3401 Silver Maple Place, Falls Church, VA 22042 <<http://www.cpcug.org/user/gabe>> (703) 204-0433



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 20

Friday 17 March 2006

Contents

- [A risk of laparoscopy](#)
[Barnaby Feder](#)
- [Security flaws could cripple missile defense network](#)
[Bob Brewin via Gabe Goldberg](#)
- [Tesco advertising SMS unsubscription requires loyalty card membership](#)
[Toby Douglass](#)
- [Elevator software risk](#)
[Toby Douglass](#)
- [When trusted systems fail](#)
[Steve Summit](#)
- [It's now a crime to delete files](#)
[Scott Peterson](#)
- [CIA Covert Agents found using fee based searches by Chicago Tribune \(R.S. Bob\) Heuman](#)
- [Another Paypal scam, social engineering against ethical people](#)
[Mark Batten-Carew](#)
- [Mindless precision](#)
[Andrew Koenig](#)

- [Re: Complexity causes 50% of product returns](#)
[Henry Baker](#)
 - [Re: Excel garbles microarray experiment data](#)
[D. McKirahan](#) [Philip Nasadowski](#) [John Deltuvia](#) [Devon McCormick](#)
 - [Australian emergency number has incorrect address information](#)
[Josh Parris](#)
 - [IEEE Symposium on Security and Privacy, Program](#)
[Cipher Editor](#)
 - [Call For Proposals: Data Surveillance and Privacy Protection workshop](#)
[Simson Garfinkel](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ A risk of laparoscopy

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

Fri, 17 Mar 2006 9:39:08 PST

To make a long story short, Kristina A. Fox received a supposedly minimally invasive laparoscopy in 1998. Unfortunately, the wand-like electrical tool that cuts tissues and seals blood vessels was emanating an undetected stray electrical charge that created a small hole in her colon. The complications resulted in 13 operations and serious complications. Her lawsuit argues that the risk of accidents from laparoscopic surgery could be sharply reduced with the use of fault-detection static and dynamic testing devices that are currently available but used by only 1/4 of U.S. hospitals. A gynecologist is quoted as saying "It wouldn't surprise me in the least if [this problem] caused more than 100 deaths and 10,000 injuries annually."

[Source: Barnaby J. Feder, Surgical Device Poses a Rare but

Serious Peril

The New York Times, 17 Mar 2006; PGN-ed; thanks to Lauren Weinstein for noting this one.]

✦ Security flaws could cripple missile defense network

<Gabe Goldberg <gabe@gabegold.com>>

Fri, 17 Mar 2006 14:34:35 -0500

The network that stitches together radars, missile launch sites and command control centers for the Missile Defense Agency (MDA) ground-based defense system has such serious security flaws that the agency and its contractor, Boeing, may not be able to prevent misuse of the system, according to a Defense Department Inspector General's report.

The report, released late last month, said MDA and Boeing allowed the use of group passwords on the unencrypted portion of MDA's Ground-based Midcourse Defense (GMD) communications network.

The report said that neither MDA nor Boeing officials saw the need to install a system to conduct automated log audits on unencrypted communications and monitoring systems. Even though current DOD policies require such automated network monitoring, such a requirement 'was not in the contract'. [...] [Source: Bob Brewin, *Federal Computing Week*, 16 Mar 2006]

<http://www.fcw.com/article92640-03-16-06-Web&newsletter%3Dyes>

Gabriel Goldberg, Computers and Publishing, Inc., 3401 Silver Maple Place,
Falls Church, VA 22042 <<http://www.cpcug.org/user/gabe>> 1-703-204-0433

✶ Tesco advertising SMS unsubscription requires loyalty card membership

<Toby Douglass <toby.douglass@summerblue.net>>
Wed, 08 Mar 2006 23:40:25 +0000

Buried deep, deep in the small print in the back pages of the Tesco (the leading UK supermarket chain) mobile phone service information booklet, is a brief sentence that if the customer wishes not to be involved in "market research", to wit, having their demographic details tracked and shared, they need to phone customer services and opt out.

Yesterday, my phone number transferred to the Tesco network and I put twenty pounds into my account.

This morning, I received an advertising SMS from Tesco.

This reminded me I needed to call customer services regarding "market research" and advertising SMSs.

Now, and here's where it gets interesting, they tell me I'm not involved in "market research" because I don't have a club card (a loyalty card) - but that for the same reason they *cannot ununsubscribe me from advertising SMSs*.

Tesco can *add* you to their advertising SMS list without a club card, but they cannot *remove* you without a club card.

What customer services do in this situation is that the shift manager visits a store, picks up a blank club card, registers it to the customer and unsubscribes them.

⚡ Elevator software risk

<"Toby Douglass" <toby.douglass@summerblue.net>>

Fri, 10 Mar 2006 14:23:56 -0000 (GMT)

I work in a three-story office block. Being so high, the building is equipped with a pair of elevators, which appear to co-operate in handling passenger traffic. These are modern elevators, equipped with a female chip-voice announcing which floor the elevator has arrived at and which direction the elevator is about to travel in.

The upper floors of the building are lightly populated and so the bathroom facilities on those floors are considerably more pleasant and less crowded.

I recently emerged from a pleasant, uncrowded bathroom and pressed the button summoning an elevator. An elevator arrived, its doors opened and a female chip voice announced the arrival of the elevator at the first floor.

The chip voice was muffled since it was coming from the *other* elevator,

which was also on the first floor with closed doors.

I stepped inside and selected "down".

The muffled other elevator announced I was about "going down" and the doors closed and the elevator took me to the ground floor.

The doors opened and the female chip voice from the floor above then floated down to me..."ground floor".

I'm grateful that it was not necessary for me to operate the controls in the other elevator. If that had been so, I wonder if the emergency button would still have worked?

When trusted systems fail

<Steve Summit <scs@eskimo.com>>

Mon, 13 Mar 2006 19:13:31 -0500

On Friday, March 10, McAfee's antivirus program gave users a nice lesson on the meaning of the term "trusted system". Due to a faulty virus definition file, the software began deleting or "quarantining" hundreds or thousands of legitimate system files (including, among others, Microsoft's excel.exe).

<http://www.realtechnews.com/posts/2802>

http://blog.washingtonpost.com/securityfix/2006/03/mcafee_update_flags_hundreds_o.html

It's now a crime to delete files

<Scott Peterson <scottp4@mindspring.com>>

Sat, 11 Mar 2006 00:20:55 -0800

What: International Airport Centers sues former employee, claiming use of a secure file deletion utility violated federal hacking laws.

When: Decided March 8 by the U.S. Court of Appeals for the 7th Circuit

Outcome: Federal hacking law applies, the court said in a 3-0 opinion written by Judge Richard Posner.

What happened, according to the court: Jacob Citrin was once employed by International Airport Centers and given a laptop to use in his company's real estate related business. The work consisted of identifying ``potential acquisition targets''.

At some point, Citrin quit IAC and decided to continue in the same business for himself, a choice that IAC claims violated his employment contract.

Normally that would have been a routine business dispute. But the twist came when Citrin dutifully returned his work laptop--and IAC tried to undelete files on it to prove he did something wrong.

IAC couldn't. It turned out that (again according to IAC) Citrin had used a ``secure delete'' program to make sure that the files were not just deleted, but overwritten and unrecoverable.

In most operating systems, of course, when a file is deleted only the reference to it in the directory structure disappears. The data

remains on the hard drive. But a wealth of programs like PGP, open-source programs such as Wipe, and a built-in feature in Apple Computer's OS X called Secure Empty Trash will make sure the information has truly vanished.

Inevitably, perhaps, IAC sued. The relevance for Police Blotter readers is that the company claimed that Citrin's alleged secure deletion violated a federal computer crime law called the Computer Fraud and Abuse Act.

That law says whoever ``knowingly causes damage without authorization'' to a networked computer can be held civilly and criminally liable.

The 7th Circuit made two remarkable leaps. First, the judges said that deleting files from a laptop counts as ``damage''. Second, they ruled that Citrin's implicit ``authorization'' evaporated when he (again, allegedly) chose to go into business for himself and violate his employment contract. ...

[URL added in archive copy;

http://news.com.com/Police+blotter+Ex-employee+faces+suit+over+file+deletion/2100-1030_3-6048449.html

]

⚡ CIA Covert Agents found using fee based searches by Chicago Tribune

<>

Sun, 12 Mar 2006 13:27:31 -0500

<http://edition.cnn.com/2006/US/03/11/cia.internet.ap/index.html>

An interesting article, reiterating what we already know, that in the present age of search tools, almost nothing can be hidden from those willing to pay for someone to do a search. The article basically says it succinctly.

✶ Another Paypal scam, social engineering against ethical people

<"Mark Batten-Carew" <markb-c@sympatico.ca>>

Mon, 13 Mar 2006 22:18:39 -0500

My wife just received what from the Subject line looked like a Paypal buyer payment notice to her, as a seller. But she hasn't recently sold anything. Having been taught to be very careful, she looked at the message source before opening it. She then checked Paypal to confirm there had been no payment to her corresponding to this message. So far so good, but now come the gotchas....

When she went to forward the message (using Outlook Express) to spoof AT paypal.com, of course the message was opened and displayed. I figured this was safe, since she would not open any attachments. But, it turns out the content of the message was a small bit of HTML, composed of just an image with a clickable area. In recent versions of IE, such images would be prevented from being downloaded unless approved. Not so in Outlook Express.

It retrieved the image, presumably identifying my wife's computer to the originating web site. Oops.

But the interesting part is that the image was a good likeness of a Paypal message, with a complete bogus transaction (to pay money to my wife) and a button to click labeled "Dispute Transaction". They are specifically preying on people who want to correct mistakes and give money back. That is, preying on ethical people, not greedy people. We didn't click on it. I have no idea what would have happened next, but probably a request to log into her account to confirm the transaction was incorrect.

⚡ Mindless precision

<"Andrew Koenig" <ark@acm.org>>

Fri, 10 Mar 2006 19:01:17 -0500

When I worked at Bell Labs, before the breakup of the Bell System in 1984, once in a while a memo would come around describing a change to some piece of hardware or other that I knew nothing about. The reason would be that the hardware was so widely used throughout the company that the easiest way to reach everyone who might care about it was to send a memo to every member of management. As an "exempt" employee, I was considered a member of management although I had no one reporting to me.

One day I received a memo that announced that as of some date, 0.511-microfarad capacitors were going to be replaced by 0.51-

microfarad capacitors, and the old ones would no longer be available.

The punchline? In both cases, the capacitors had +/- 10% tolerance.

[Unfortunately, the capacity of management often has a tolerance greater than +/- 10%. PGN]

⚡ Re: Complexity causes 50% of product returns ([RISKS-24.19](#))

<Henry Baker <hbaker1@pipeline.com>>

Thu, 16 Mar 2006 13:14:16 -0800

This problem affects more than consumer devices. When I was working on a project for the Army in the very early 1970's regarding repairing tank engines, a significant fraction (1/4 - 1/3) of tank engines that were sent back from Viet Nam had "nothing wrong" with them. (I don't know how they came up with this statistic -- we've all gotten our cars back from the repair shop, only to find that the problem that we took the car into the shop for in the first place had not been fixed.)

Of course, a number of the broken engines had been "hacked" -- i. e., "hot-rodged" by some good ol' boys, so they failed in a sometimes spectacular manner. But that is a different story...

Re: Excel garbles microarray experiment data ([RISKS-24.19](#))

<"D. McKirahan" <dmckirahan@comcast.net>>

Fri, 10 Mar 2006 17:05:23 -0600

Frequent users of MS-Excel know to format the cells as Text
before
entering data or put a single quote in front of any data to have
it stay
as-is.

```
'1DEC                won't change to      01-Dec  
'2310009E13        won't change to      2.31E+19
```

Re: Excel garbles microarray experiment data ([RISKS-24.19](#))

<Philip Nasadowski <nasadowsk@usermail.com>>

Sun, 12 Mar 2006 15:12:43 -0500

I'm glad (well, not really) I'm not the only one who's seen
their data
swallowed by Excel. I have seen this with data provided by a
custom
application for a 'large northeastern USA transit operator'.
Basically,
there's certain data that's represented in hexadecimal format.
When the
output file (comma separated values, csv) is brought into Excel,
Excel
'helpfully' converts some of these into scientific notation!
And you can't
turn it off or unformat it, period. It's converted and that's
that. I
haven't bothered calling MS, representing data as typed is
apparently too
advanced a concept for them to understand...

At least what we're looking at isn't super critical, and Excel is only one tool that we use. The scary thing, though, is there's no warning, and you can't turn it off. Who knows what other liberties MS takes with your data...

⚡ Re: Excel garbles microarray experiment data ([RISKS-24.19](#))

<John.Deltuvia@judiciary.state.nj.us>

Mon, 13 Mar 2006 09:52:05 -0500

I do not see this as a problem in Excel, which is a spreadsheet program designed primarily for accounting calculations - calculations which commonly use numbers and dates.

Rather, this is a problem introduced by the designer(s) of the "new bioinformatics programs", who seem to have decided to use Excel as a database program. A crowbar can be used as a hammer, but one runs the risk of making a large hole in a wall instead of simply driving in the nail. Similarly, using Excel as a database instead of Oracle, or SQL Server, or even MS Access (if for some reason use of the MSOffice suite is desired) runs the risk of non-accounting data being interpreted as accounting data.

John J. Deltuvia, Jr, Technology Unit, NJAOC Probation Services
- CSES

✉ **Re: Excel garbles microarray experiment data ([RISKS-24.19](#))**

<"Devon McCormick" <devonmcc@gmail.com>>

Mon, 13 Mar 2006 15:54:30 -0500

Excel doesn't play well with others. This is not the only kind of data Excel garbles.

In the financial world, we use CUSIPs (8 or 9 character codes) or tickers (1- to 5-letter codes) to identify equities. Excel typically garbles these by being over-helpful as mentioned in the article on micro-array data. So, CUSIPs are sometimes left alone and often treated as numbers because they are a mix of letters and numerals with the a preponderance of numerals. Tickers are less commonly mangled though there is a company with the ticker "TRUE" which Excel decides is the value "TRUE", not the character string.

However, potentially even more insidious is the fact that Excel does not properly handle .CSV files. This "Comma-Separated Values" format has been around for decades but Excel has never handled it properly. Both on input and output, it will often ignore the double-quotes that are intended to distinguish character from numeric fields.

Because of this, the obvious solution of putting CUSIPs and tickers in quotes does not work with Excel.

Perhaps even worse, there are applications that expect the Excel variant of

.CSV files and reject properly-formatted ones. To see how ridiculously complicated this can get, look at the section "Excel vs. Leading Zero & Space" in <http://www.creativyst.com/Doc/Articles/CSV/CSV01.htm#CSVVariations>.

Thus the risk of the popular error propagating, muddying the waters for years to come.

⚡ Australian emergency number has incorrect address information

<Josh Parris <josh_parris@win32dev.com>>

Tue, 14 Mar 2006 10:18:42 +1100

The local emergency number, 000, is reported to have incorrect address information:

<http://theage.com.au/news/NATIONAL/Telstra-to-upgrade-Triple0-database/2006/03/14/1142098425868.html>

There is no media release on the Telstra website relating to this.

⚡ IEEE Symposium on Security and Privacy, Program

<"Cipher Editor" <cipher-editor@ieee-security.org>>

Fri, 17 Mar 2006 10:46:53 -0700

The Symposium will be held May 21-24 at the Claremont Resort in Berkeley,

California. See <http://www.ieee-security.org/TC/SP2006/oakland06.html>

Session: Signature Generation (Christopher Kruegel)

Towards Automatic Generation of Vulnerability-Based Signatures
David Brumley, James Newsome, Dawn Song, Hao Wang, and Somesh Jha
Carnegie Mellon University, USA, and University of Wisconsin, USA

Misleading Worm Signature Generators Using Deliberate Noise Injection

Roberto Perdisci, David Dagon, Wenke Lee, Prahlad Fogla, and Monirul Sharif
University of Cagliari, Italy, and Georgia Institute of Technology, USA

Hamsa: Fast Signature Generation for Zero-day Polymorphic Worms
with Provable Attack Resilience

Zhichun Li, Manan Sanghi, Yan Chen, Ming-Yang Kao and Brian Chavez
Northwestern University, USA

Session: Detection (Robert Cunningham)

Dataflow Anomaly Detection

Sandeep Bhatkar, Abhishek Chaturvedi and R. Sekar
Stony Brook University, USA

Towards a Framework for the Evaluation of Intrusion Detection Systems

Alvaro A. Cardenas, Karl Seamon and John S. Baras
University of Maryland, USA

Siren: Detecting Evasive Malware (Short Paper)

Kevin Borders, Xin Zhao and Atul Prakash
University of Michigan, USA

Session: Privacy (Carl Landwehr)

Fundamental Limits on the Anonymity Provided by the MIX Technique
Dakshi Agrawal, Dogan Kesdogan, Vinh Pham, Dieter Rautenbach
IBM T J Watson Research Center, USA, RWTH Aachen, Germany,
and University of Bonn, Germany

Locating Hidden Servers

Lasse O/verlier and Paul Syverson

Norwegian Defence Research Establishment, Norway, Gjøvik
University

College, Norway, and Naval Research Laboratory, USA

Practical Inference Control for Data Cubes (Extended Abstract)

Yingjiu Li, Haibing Lu and Robert H. Deng

Singapore Management University, Singapore

Deterring Voluntary Trace Disclosure in Re-encryption Mix
Networks

Philippe Golle, Xiaofeng Wang, Markus Jakobsson and Alex Tsow

Palo Alto Research Center, USA, and Indiana University,
Bloomington, USA

New Constructions and Practical Applications for Private Stream
Searching (Extended Abstract)

John Bethencourt, Dawn Song and Brent Waters

Carnegie Mellon University, USA, and SRI International, USA

5-minute Work-in-Progress Talks

Session: Formal Methods (Susan Landau)

A Computationally Sound Mechanized Prover for Security Protocols

Bruno Blanchet

CNRS, Ecole Normale Supe'rieure, Paris, France

A Logic for Constraint-based Security Protocol Analysis

Ricardo Corin, Ari Saptawijaya and Sandro Etalle

University of Twente, The Netherlands, and University of
Indonesia, Indonesia

Simulatable Security and Concurrent Composition

Dennis Hofheinz and Dominique Unruh

CWI, The Netherlands, and University of Karlsruhe, Germany

Session: Analyzing and Enforcing Policy (Tuomas Aura)

Privacy and Contextual Integrity: Framework and Applications

Adam Barth, Anupam Datta, John C. Mitchell and Helen Nissenbaum

Stanford University, USA, and New York University, USA

FIREMAN: A Toolkit for FIREwall Modeling and ANalysis

Lihua Yuan, Jianning Mai, Zhendong Su, Hao Chen, Chen-Nee Chuah
and

Prasant Mohapatra

University of California, Davis, USA

Retrofitting Legacy Code for Authorization Policy Enforcement

Vinod Ganapathy, Trent Jaeger and Somesh Jha

University of Wisconsin-Madison, USA,

and Pennsylvania State University, USA

Session: Analyzing Code (Doug Tygar)

Deriving an Information Flow Checker and Certifying Compiler for
Java

Gilles Barthe, David A. Naumann and Tamara Rezk

INRIA Sophia-Antipolis, France, and Stevens Institute of
Technology, USA

Discovering Malicious Disks with Symbolic Execution

Paul Twohey, Junfeng Yang, Can Sar, Cristian Cadar, and Dawson
Engler

Stanford University, USA

Pixy: A Static Analysis Tool for Detecting Web Application
Vulnerabilities

Nenad Jovanovic, Christopher Kruegel and Engin Kirda

Vienna University of Technology, Austria

Cobra: Fine-grained Malware Analysis using Stealth Localized-
Executions

Amit Vasudevan and Ramesh Yerraballi

University of Texas Arlington, USA

Session: Authentication (Paul Van Oorschot)

Integrity (I) codes: Message Integrity Protection and
Authentication

Over Insecure Channels

Mario Cagalj, Srdjan Capkun, Ramkumar Rengaswamy,

Ilias Tsigkogiannis, Mani Srivastava and Jean-Pierre Hubaux

Ecole Polytechnique Federale de Lausanne (EPFL), Switzerland,
Technical University of Denmark, Denmark,
and University of California, Los Angeles, USA

Cognitive Authentication Schemes Safe Against Spyware
Daphna Weinshall, Hebrew University of Jerusalem, Israel

Cache Cookies for Browser Authentication (Extended Abstract)
Ari Juels, Markus Jakobsson and Tom N. Jagatic
RSA Laboratories, USA, RavenWhite Inc., USA, and Indiana
University, USA

Secure Device Pairing based on a Visual Channel
Nitesh Saxena, Jan-Erik Ekberg, Kari Kostiainen and N. Asokan
University of California, Irvine, USA, and Nokia Research
Center, Finland

Session: Attacks (Kevin Fu)

SubVirt: Implementing malware with virtual machines
Samuel T. King, Peter M. Chen, Yi-Min Wang, Chad Verbowski,
Helen J. Wang,
Jacob R. Lorch, University of Michigan, USA, and Microsoft
Research, USA

Practical Attacks on Proximity Identification Systems (Short
Paper)
Gerhard P. Hancke, University of Cambridge, UK

On the Secrecy of Timing-Based Active Watermarking Trace-Back
Techniques
Pai Peng, Peng Ning and Douglas S. Reeves, North Carolina State
University, USA

Session: Systems (Helen Wang)

A Safety-Oriented Platform for Web Applications
Richard S. Cox, Jacob Gorm Hansen, Steven D. Gribble, and Henry
M. Levy
University of Washington, USA, and University of Copenhagen,
Denmark

Tamper-Evident, History-Independent, Subliminal-Free Data

Structures

on PROM Storage -or- How to Store Ballots on a Voting Machine
(Extended Abstract)

David Molnar, Tadayoshi Kohno, Naveen Sastry and David Wagner
University of California, Berkeley, USA, and University of
California,
San Diego, USA

Analysis of the Linux Random Number Generator

Zvi Gutterman, Benny Pinkas and Tzachy Reinman

Hebrew University, Israel, Haifa University, Israel, and Safend,
Israel

The Final Nail in WEP's Coffin

Andrea Bittau, Mark Handley and Joshua Lackey

University College London, UK, and Microsoft, USA

Call For Proposals: Data Surveillance and Privacy Protection workshop

<Simson Garfinkel <simsong@acm.org>>

Sat, 11 Mar 2006 17:03:05 -0500

CRCS Workshop 2006: Data Surveillance and Privacy Protection

- * Can you find the terrorist in your database?
- * Do hospital admission records hold the secret to catching and confining Avian Flu outbreaks in humans?
- * What do banks really know about their customers?
- * What's the real purpose behind that RFID tag on your sweater?

On June 3, 2006 Harvard University's Center for Research on
Computation and

Society will hold a day-long workshop on Data Surveillance and
Privacy
Protection.

Although there has been significant public attention to the

civil liberties
issues of data surveillance over the past few years, there has
been little
discussion of the actual techniques that could be employed in
any but the
most restricted settings. Likewise, there has been little
discussion of
methods and technologies for conducting data surveillance while
respecting
privacy and preserving civil liberties.

Today's newspapers and TV shows are preoccupied with NSA
wiretaps and the
accidental release of names and social security numbers.
Meanwhile, a far
more pervasive surveillance infrastructure is being created
around us: the
routine use of database information for law enforcement, counter-
terrorism,
and commercial markets.

The Center for Research on Computation and Society (CRCS) is a
new research
center with a mission to develop a clear understanding of issues
of
technology and public policy where the actual technology makes a
difference,
and to pursue innovative computer science and technology
research informed
by that understanding.

Some of the issues that we would like to explore at the workshop
include:

- * Techniques for mining databases within and between
organizations without
exposing proprietary or privacy-sensitive information.
- * Techniques that are planned for deployment (or are actually
being used) to
survey hospital admissions data for evidence of epidemics or
bioterror
attacks.

* Techniques that have been tried, or proposed, for finding terrorists or criminals through the examination of transactional information.

* Techniques that could be used to automatically detect phishing attacks or other kinds of financial fraud.

The workshop will take place on June 3, 2006. Registration for the workshop will open in early May.

CALL FOR PAPERS AND PRESENTATIONS

The CRCS Workshop Organizing Committee is looking for academics, government officials, business leaders, and individuals who are interested in submitting papers or making presentations at the June 3rd workshop. If you are interested, please send us a 2-paragraph abstract of your proposed paper or presentation.

Send proposals to crcs-wkshp06@eecs.harvard.edu

For more information, check out wiki at: http://www.eecs.harvard.edu/crcs/wiki/index.php/Spring_2006_Workshop_CFP



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 21

Thursday 23 March 2006

Contents

- [More SAT errors](#)
[Jeremy Epstein](#)
- [Texas voting recount halted](#)
[David Lesher](#)
- [Baby dies after untrained doctor presses wrong button](#)
[Adam Hupp](#)
- [Tax Data for Sale?](#)
[Chris Hoofnagle](#)
- [Fidelity laptop with customer data stolen](#)
[Bob Heuman](#)
- [Fidelity loses laptop, recovery effort looks like phish](#)
[Larry Stewart](#)
- [Risks: adoption vs. abortion?](#)
[Harry Hochheiser](#)
- [How risky are preapproved credit card applications?](#)
[Steve Summit](#) [Mark Brader](#)
- [Re: Crime to Delete Files](#)
[Sidney Markowitz](#)

- [Re: Excel garbles microarray experiment data](#)
[Fernando Pereira](#) [Dimitri Maziuk](#) [Tim Duncan](#) [Nick Malcolm](#) [Olaf Seibert](#)
 - [Risks of frequent publication](#)
[Rob Slade](#)
 - [OSDI '06 CfP](#)
[Geoff Voelker](#)
 - [Call for Participation - Team Software Process Symposium](#)
[Carol Biesecker](#)
 - [REVIEW: "Network Security Tools", Nitesh Dhanjani/Justin Clarke](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ More SAT errors

<Jeremy Epstein <jeremy.epstein@webmethods.com>>

Thu, 23 Mar 2006 06:59:42 -0800

In [RISKS-24.19](#), there were three reports about the College Board reporting problems with SAT scoring. First, the College Board said that about 4000 tests were misgraded, with results off by no more than 100 points. Then the College Board admitted some were off as much as 200, or maybe even 400 points (out of 2400 total).

Today, the College Board admits that there were an additional 27,000 score sheets that weren't rechecked, and they found 375 more students who received incorrect scores. There was no disclosure of how far off these results were. The article notes "The College Board said that from now on all answer sheets would be scanned twice, among other new precautions, and that it

would retain consulting firm Booz Allen Hamilton to perform a comprehensive review within 90 days."

(<http://www.cnn.com/2006/EDUCATION/03/23/sat.scoring.error.ap/index.html>)

Two things struck me about this sequence of revelations:

(1) Does the College Board even have a *legal* obligation to disclose this information? Could it be that this has happened in the past, and without the increased scrutiny caused by the disclosures of personal information leakage, they might never have told the students or the public?

(2) On the positive side, it's a good thing there's paper to double-check.

If these were votes on paperless DREs instead of SAT scores, there would be no way of knowing that they had been miscounted.

As a parent whose oldest child went through the process last year, I'm relieved that she's not having to deal with this headache - and I feel sorry for any student who made decisions on where to apply based on SAT scores.

(I know we used my daughter's scores to help find target schools - if they had been off by a few hundred points, she might not even have applied to the school she selected.) While colleges can reexamine the applications in light of corrected SAT scores, there's nothing that can be done for applications that weren't submitted based on incorrect results.

Karen W. Arenson in *The New York Times* today is reporting that the College Board has now admitted that the maximum error was 450 points (out of 2400).

The College Board had previously claimed 100, then 200, then

400. Her
article included this wonderful quote:

"Everybody appears to be telling half-truths, and that erodes confidence in the College Board," said Bruce J. Poch, vice president and dean of admissions at Pomona College in Claremont, Calif. "It looks like they hired the people who used to do the books for Enron. My next question is what other surprise we're going to hear about next."

[http://www.nytimes.com/2006/03/23/education/23sat.html?
_r=1&oref=slogin](http://www.nytimes.com/2006/03/23/education/23sat.html?_r=1&oref=slogin)

[Lauren Weinstein noted that in its statement, the Board said Pearson would ensure that all answer sheets were "acclimatized before scanning" and would scan each answer sheet twice. Pearson will also improve its software to detect whether answer sheets have expanded because of humidity. PGN]

[Jeremy's point about the paperless DREs is apt, but this case reminds us once again that even paperfull media such as optical scanning can have serious problems that require oversight and the willingness to perform meaningful recounts -- which are of course impossible with the current breed of paperless DREs. PGN]

Texas voting recount halted

<David Leshner <lesher@epic.org>>

Wed, 22 Mar 2006 18:16:21 -0500

Court-at-law recount suspended; Electronic machines not providing all info

Paul A. Anthony, 21 Mar 2006

On orders from the Texas Secretary of State's office, the recount for the Tom Green County Court-at-Law No. 2 race has been suspended midway through its second day. About 1:30 p.m. today, county Republican Chairman Dennis McKerley stopped the recount after workers found discrepancies of as much as 20 percent between what was counted Monday and what was reported Election Night. "We're having some trouble with the electronic equipment," McKerley said. Apparently, McKerley said, new electronic voting machines provided by vendor Hart InterCivic are not printing ballots for every vote cast on the machines. During recounts, which must be done by hand, the machines are designed to print out separate ballots for every vote. http://www.sanangelostandardtimes.com/sast/news_local/article/0,1897,SAST_4956_4559073,00.html

⚡ Baby dies after untrained doctor presses wrong button

<Adam Hupp <hupp@upl.cs.wisc.edu>>

Tue, 21 Mar 2006 09:17:49 -0600

"A baby boy died after an untrained doctor pressed the wrong button on his bypass machine because it was a less 'horrid' colour than the other, an

inquest heard yesterday. ... [The doctor] was unaware how to use the machinery, as were most of the team."

<http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/03/21/nhs121.xml>

✦ Tax Data for Sale?

<Chris Hoofnagle <hoofnagle@epic.org>>

Wed, 22 Mar 2006 08:39:21 -0800

"The *Philadelphia Inquirer* reports that the IRS has proposed rule changes

allowing tax-return preparers, like H&R Block, to sell an individual's

return information to marketers and data brokers. The proposed rule,

which does contain some substantive protections for the processing of

electronic returns, was published in the Federal Register on December 8,

2005. The official comment period has passed, but hearings will be held

this month." [<http://rss.slashdot.org/slashdot/eqWf?m=4398>]

Well, kind of. Under the new rule, disclosure of tax return information is

broadened if the customer gives her affirmative consent. If consent is

given, the FULL RETURN can be given to other entities for marketing

purposes, and the tax preparer does not have to even ensure that these other

entities are legit or following the preparer's privacy policy.

I'm basically telling people not to use storefront tax preparation at all,

because if they don't trick you into selling your data, they'll

use it themselves to market bogus refund anticipation loans. Unfortunately, even the tax preparation software tries to market that to you now.

[Added note: The current rule allows sharing with affiliates if the consumer gives opt-in consent. The new rule expands sharing to any third party, but requires a more explicit opt-in. However, once the data are shared, the preparer has no responsibilities for how it is used.]

✶ Fidelity laptop with customer data stolen

<Bob Heuman <rsh@idirect.com>>
Thu, 23 Mar 2006 14:00:43 -0500

This one seems to impact Hewlett Packard employees in the U.S. - I do not know if those in Canada and elsewhere in the world are impacted. No word on use of encryption to protect the data, so I suspect it was NOT protected at all. Will they ever learn?

A laptop computer belonging to Fidelity Investments and containing sensitive data on about 196,000 retirement-account customers was stolen last week, the company said.
http://www.usatoday.com/money/industries/brokerage/2006-03-23-fidelity_x.htm

✶ Fidelity loses laptop, recovery effort looks like phish

<Larry Stewart <larry@stewart.org>>

Wed, 22 Mar 2006 19:27:01 -0500

Evidently Fidelity lost a laptop containing the HP retirement records.

No explanation why it was reasonably on said laptop.

To their credit, they sent UPS letters to everyone, but:

- a) The letters contain an 800 number to call
- b) The 800 number wants you to key in your social security number before talking to a person.

Well that is not a very good design!

At least the folks at the main Fidelity number knew how to confirm the special number.

I was calling to tell them I got someone else's letter at my address in addition to my own, but I was seriously surprised by the "enter ssn".

I would note:

- Poor security practices (data on laptops)
- Inability to learn from other companies previous misfortunes
- + An apparently serious response
- A poorly designed response
- Bad database data - will I get this fellow's pension too?

✶ Risks: adoption vs. abortion?

<Harry Hochheiser <harry@alum.mit.edu>>

Tue, 21 Mar 2006 07:33:11 -0500

Here's another example of problems with automated language processing.

<http://www.wired.com/news/wireservice/0,70453-0.html?tw=rss.technology>

Amazon Changes 'Abortion' Queries

Amazon.com said Monday it had modified the way its search engine handles queries for the term "abortion" after receiving an e-mail complaint that the results appeared biased. Until the recent change, a user who visited the Seattle Internet retailer and typed in the word "abortion" received a prompt asking, "Did you mean adoption?" followed by search results for "abortion."

Spokeswoman Patty Smith said the automated prompt was purely based on technology, and that no human had made the decision to show the question.

"Adoption and abortion are the same except for two keystrokes," Smith said. "They also, in this case, happen to be somewhat related terms."

Still, Smith said she and other company officials decided to remove the question after receiving an e-mail complaint and deciding that it raised a valid concern.

People who type in the term "adoption" do not see a prompt asking "Do you mean abortion?"

✦ How risky are preapproved credit card applications?

<Steve Summit <scs@eskimo.com>>

Thu, 16 Mar 2006 16:44:46 -0500

If you're concerned about privacy, you may be worried about merely throwing away those preapproved credit card applications that come in the mail, especially when they're pre-filled with your name and other information. Indeed, the Federal Trade Commission and many banks recommend tearing up those applications before discarding them. But Rob Cockerham, my favorite empiricist, decided to test how well that strategy actually works. He tore up an application, taped it back together, and mailed it in. Did the bank process the application and issue him a card anyway? One guess. <http://www.cockeyed.com/citizen/creditcard/application.shtml>

✦ Re: How risky are preapproved credit card applications?

<msb@vex.net (Mark Brader)>

Thu, 16 Mar 2006 17:05:00 -0500 (EST)

> He tore up an application, taped it back together, and mailed it in.

Ahem. He tore up an application, taped it back together, filled it out

with a change of address requested, and mailed it in.

✉ **Re: Crime to Delete Files ([RISKS-24.20](#))**

<Sidney Markowitz <sidney@sidney.com>>

Sat, 18 Mar 2006 14:08:45 +1300

The spin on the story in [RISKS-24.20](#) was "how awful that a judge says it's illegal to use a secure delete program." But how is this different from a disgruntled employee shredding the only copy of paper files of valuable customer information before quitting to start his own business in competition with his former employer?

It should make a difference, of course, whether the deleted files were valuable to the company, and if they were the only copy of the information. The ex-employee made the additional argument that his employment contract specified that he was to return or destroy data upon leaving the company. The company asserted that he had broken the contract and so those the authorization implied by those terms were no longer in force.

But the story reports that this was an appeals case. Based on the story, it appears that the judge did not say that files were deleted illegally, only ruled there could be facts in the case which would cause the deletions to be considered as damage and unauthorized. The case was sent back to the lower court so that these facts could be determined.

Sidney Markowitz <http://www.sidney.com>

✉ **Re: Excel garbles microarray experiment data (Deltuvia, [RISKS-](#)**

24.19)

<Fernando Pereira <pereira@cis.upenn.edu>>

Sat, 18 Mar 2006 01:43:32 -0500

Here's Microsoft's own description of Excel from online book that came with my copy of the software:

```
> Microsoft® Excel 2004 for Mac®
> Use this analysis and spreadsheet program to evaluate,
calculate, and
> analyze data. Make use of the improved charting and page layout
> capabilities to illustrate your data and make it look good in
print.
```

An "analysis" program, designed to "analyze data". No mention of accounting. For a scientist, to "analyze data" involves computing statistical summaries and plotting, not silent conversions of data

labels. Furthermore, I don't think the work in question used Excel as a database program, but rather as a program to analyze the results of microarray experiments. This task is entirely within the job description for Excel quoted above.

✶ **Re: Excel garbles microarray experiment data ([Risks-24.20](#))**

<dmaziuk@bmrw.wisc.edu (Dimitri Maziuk)>

Sat, 18 Mar 2006 13:26:15 -0600

Re: Deltuvia

Actually, if you follow the references in the original article, both

bioinformatics programs are written in Java with SQL back-ends.

"Tab-delimited file suitable for loading into spreadsheet

programs" is one
of their listed output options.

So the problem was introduced by the authors of the original
report when
they decided to load those output files into Excel for viewing.

Re: McCormick"

> ... it will often ignore the double-quotes that are intended to
distinguish character from numeric fields.

Yes, it does that. Note, however, that there is no standard for
CSV
format. Some applications allow special characters (such as
newlines: record
separator) inside double-quoted values, some don't. Some
applications
escape a double quote inside double-quoted values with a
backslash
(C-style), some use a second quote (SQL-style), some simply
can't handle
it. There is no way to disambiguate non-text values, such as
20060318. MySQL
outputs null fields as ",\N," whereas most others do just ",,".
And so on.

Which is not as bad as tab-delimited files (output of the two
bioinformatics
programs in question) where on top of all of the above, a single
tab may
replaced by 8 (or some other number) of consecutive spaces and
there is an
option to "not treat consecutive spaces as one". (I.e. to treat
"\t\t" as a
null field.) Of course, to most parsers a whitespace is just a
whitespace,
be it "\t" or a " ", so the end result is you get 8 extra null
columns
because you previously looked at the file in some helpful text
editor that
quietly replaced tabs with spaces for your viewing pleasure.

✉ Re: Excel garbles microarray experiment data ([RISKS-24.19](#))

<<tim.duncan@duncan.cx>>

Sat, 18 Mar 2006 19:32:36 -0800

My company often gives clients data in CSV formatted file that doesn't end in .CSV. This data is usually imported into an accounting system but sometimes users want to look it over in Excel (if it isn't in Excel it isn't data to some people) so they open Excel and then open the file thus bringing up the "Text Import Wizard". The wizard is pretty straight forward, you select delimited then select comma as your delimiter and click Finish. Here is the catch; Excel brings all the columns in using the "General" format, not the "Text" format unless you specify this on the last screen (3 of 3) of the wizard which is often skipped. Thus data that starts with a zero or has a lone 'E' with numbers is often mis-represented. You would think that data brought in via a TEXT Import Wizard would be treated as text but unfortunately this is not the case.

✉ Re: Excel garbles microarray experiment data

<nick.malcolm@gb.abb.com>

Mon, 20 Mar 2006 15:44:17 +0000

While working on a joint UK / German product development we discovered that

the 'standard' separator employed in many German CSV files is the semi-colon

';' - I do not know why.

This property is defined in the Regional and Language Options of the Machine

as described in the Microsoft Excel Help (in case anyone should need it) :

Change the separator in a CSV text file

1. Click the Windows Start menu.
2. Click Control Panel.
3. Open the Regional and Language Options dialog box.
4. Click the Regional Options Tab.
5. Click Customize.
6. Type a new separator in the List separator box.
7. Click OK twice.

Note After you change the list separator character for your machine, all

applications will use the new character. You can change the character back

to the original character by using the same procedure.

Naturally, on my machine (Windows 2000) the above 'Help' was found like this:

Change the separator in a CSV text file

1. Click the Windows Start menu.
2. Click Control Panel.
3. Open the Regional Options dialog box.
4. Click the Numbers Tab.
5. Click Customize.
6. Type a new separator in the List separator box.
7. Click OK twice once.

Re: Excel garbles microarray experiment data ([RISKS-24.19](#))

<Rhialto <rhialto@falu.nl>>

Thu, 23 Mar 2006 14:30:06 +0100

For example, the RIKEN identifier "2310009E13" was converted irreversibly to the floating-point number "2.31E+13."

That should have been 2.31E+19. Error of the original author, or even further error of Excel?

(the original page doesn't seem to offer access to the e-mail addresses;
I had wanted to copy the authors too)

Olaf 'Rhialto' Seibert rhialto/at/xs4all.nl

✦ Risks of frequent publication

<Rob Slade <rMslade@shaw.ca>>
Wed, 22 Mar 2006 20:37:01 -0800

Copyright Gone Mad (copyright Robert M. Slade, 2006)
(with that little (c) symbol thrown in for good measure)

I got asked to do a 20-year retrospective on computer viruses for a tech magazine. There were a few oddities about the request, such as a demand for graphics. I normally don't do graphics, but I had such a fun time doing the article that I gave in, and finally put together quite a piece, I thought. It was a gas going back over all the stuff I've seen over the years.

You may never see it.

See, I got this phone call from the magazine today. It seems that some of the wording in my article bears a striking resemblance to a site

on the
Internet: "Robert Slade's Computer Virus History" at
<http://www.cknow.com/vtutor/RobertSladesComputerVirus.html>.

This is surprising?

I've been writing articles, series, and books about viruses since the darn things started. As a matter of fact, it's a bit surprising that they didn't find more sites with my stuff on it, especially since there have been dozens of examples that I've seen myself, over the years, where people have used my material and passed it off as their own.

But it seems that this outfit has a policy where they won't publish anything that has already appeared on the net.

I suppose that's fair enough. Everybody is getting really antsy about copyright violations these days, and, as somebody who does an awful lot of writing, I suppose I should approve.

Except I don't. The crackdown (and crankdown) on copyright and copying is making it hard for a lot of us who are relying on our own research and writing. After all, who else am I going to use for material on virus history? Oh, lots of people were there, but who else wrote it down? I do go back (and did go back, for this article) and check on specifics, and even made corrections on items we've found out more about. But, by and large, if I want to generate a decent timeline of what happened, I have to rely very heavily on my own stuff.

Except, now I can't.

Well, like I said, you may not get to see the history article.
Or, if they
are willing to bend their policy a bit, you might. But I'm
willing to bet
that their policy is more important to them. After all, they
can always get
another writer to do it for them.

Of course, in all probability he won't know anything about the
history of
viruses.

Or, he can read my stuff. And reuse it.

copyright Robert M. Slade, 2006

(with that little (c) symbol thrown in for good measure)

rslade@vcn.bc.ca

slade@victoria.tc.ca

rslade@sun.soci.

niu.edu

<http://victoria.tc.ca/techrev>

or

<http://sun.soci.niu.edu/>

[~rslade](http://sun.soci.niu.edu/~rslade)

[Ironic. I keep Robert's copyright line in his reviews,
despite the RISKS

info file that once upon a time said that by default
everything that

appears in RISKS is fair game if used with appropriate
credits. I just

discovered that the relevant wording in the risksinfo file
somehow got

deleted somewhen along the way, and I suppose I'd better fix
that. Or

perhaps it is better to leave it unspecified so that others
can quote

Robert without his permission! PGN]

OSDI '06 CFP

<Geoff Voelker <voelker@CS.UCSD.EDU>>

Wed, 22 Mar 2006 22:18:37 -0800

OSDI '06 Call for Papers [Adapted for RISKS by PGN]
7th Symposium on Operating Systems Design and Implementation
(OSDI '06)

Seattle, WA, USA, November 6-8, 2006,
Sponsored by USENIX, in cooperation with ACM SIGOPS
<http://www.usenix.org/events/osdi06/cfp/>

The seventh OSDI seeks to present innovative, exciting work in the systems area ... on the design, implementation, and implications of systems software. The OSDI Symposium emphasizes both innovative research and quantified or illuminating experience. OSDI takes a broad view of the systems area and solicits contributions from many fields of systems practice, including, but not limited to, operating systems, file and storage systems, distributed systems, mobile systems, secure systems, embedded systems, networking as it relates to operating systems, and the interaction of hardware and software development. We particularly encourage contributions containing highly original ideas, new approaches, and/or groundbreaking results. [Full papers are due by 24 Apr 2006.]

Call for Participation - Team Software Process Symposium

<cb@sei.cmu.edu (Carol Biesecker)>
Thu, 23 Mar 2006 19:29:26 +0000 (UTC)

Team Software Process Symposium
18-20 Sep 2006, Omni Hotel, San Diego, California

Web: <http://www.sei.cmu.edu/tsp/symposium.html>

Theme: Measurable Improvements in Team Performance

Deadline for abstracts 28 Apr 2006

The first Team Software Process (TSP) Symposium will include all yearly TSP activities. The conference will bring together users, adopters, and developers of the TSP, those involved in its development and transition, and those who are new to the technology and eager to learn more. Attendees will have the opportunity to exchange ideas, concepts, and lessons learned concerning the experiences, best practices, and suggested introduction strategy for the TSP methods and practices.

**** All inquiries to jsn@sei.cmu.edu ****

Jodie Spielvogel, TSP Team

Software Engineering Institute, 4500 Fifth Avenue, Pittsburgh, PA 15213

Phone: 412 / 268-6504 FAX: 412 / 268-5758 E-mail: jsn@sei.cmu.edu

REVIEW: "Network Security Tools", Nitesh Dhanjani/Justin Clarke

<Rob Slade <rMslade@shaw.ca>>

Tue, 21 Mar 2006 10:48:31 -0800

BKNTSCTL.RVW 20051204

"Network Security Tools", Nitesh Dhanjani/Justin Clarke, 2005, 0-596-00794-9, U\$34.95/C\$48.95

%A Nitesh Dhanjani

%A Justin Clarke

%C 103 Morris Street, Suite A, Sebastopol, CA 95472

%D 2005

%G 0-596-00794-9
%I O'Reilly & Associates, Inc.
%O U\$34.95/C\$48.95 800-998-9938 fax: 707-829-0104 nuts@ora.com
%O [http://www.amazon.com/exec/obidos/ASIN/0596007949/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0596007949/robsladesinterne)
[http://www.amazon.co.uk/exec/obidos/ASIN/0596007949/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0596007949/robsladesinte-21)
%O [http://www.amazon.ca/exec/obidos/ASIN/0596007949/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0596007949/robsladesin03-20)
%O Audience a- Tech 2 Writing 1 (see revfaq.htm for
explanation)
%P 324 p.
%T "Network Security Tools"

The preface states that the audience for the book is comprised of anyone who wants to program their own vulnerability scanners, or extend those already available. It assumes familiarity with six of the major tools in that class, as well as Perl.

Chapter one deals with writing plug-ins for Nessus. It covers the installation and quick use of the program, and then outlines the Nessus Attack Scripting Language, including a few sample scripts. The Ettercap network analyzer and its plug-ins (in the C language) are in chapter two. (An overview of authentication for the ftp protocol is provided in order to discuss looking for ftp passwords.) The Hydra password sniffer (and SMTP authentication) is described in chapter three, as well as the Nmap port scanner. Chapter four looks at plug-ins (in Perl) for the Nikto Web scanner. The Metasploit Framework generic exploit development platform is examined in chapter five, which also has a brief explanation of stack overflows. Chapter six discusses analysis of (mostly source) code for Web applications in a search for vulnerabilities, reviewing the PMD Java analysis

tool,
and reprinting pages of Java source code.

Part two turns to writing network security tools. Chapter seven is primarily a tutorial on Linux kernel modules. Using Perl to write a Web application scanner is in chapter eight. SQL injection, and testing for error message responses, is examined in chapter nine. Chapter ten covers the use of the libpcap library for producing network sniffing utilities. Packet injection, using the libnet library and AirJack device driver, is in chapter eleven.

While a lot of sample code is given in this text, ultimately it is about using a bunch of tools. The examples and exploits are interesting, and do provide an indication of limited types of testing utilities that could be developed.

copyright Robert M. Slade, 2005 BKNTSCTL.RVW 20051204
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.
niu.edu
http://victoria.tc.ca/techrev or [http://sun.soci.niu.edu/
~rslade](http://sun.soci.niu.edu/~rslade)



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 22

Saturday 1 April 2006

Beware April Foolishness

Contents

- [Motorist trapped in traffic circle for 14 hours](#)
[Don Norman](#)
- [Airbus A380 Evacuation Test](#)
[Peter B. Ladkin](#)
- [Boeing B777 flight control anomalies](#)
[Peter B. Ladkin](#)
- [Cartography dream realized](#)
[Don Norman](#)
- [On the SAT errors](#)
[PGN](#)
- [Re: More SAT errors](#)
[Richard Outerbridge](#) [Steve Schafer](#)
- [Man is charged \\$4,334.33 for four burgers](#)
[PGN](#)
- [Offshore outsourcing cited in Florida data leak](#)
[Robert McMillan](#)

- [City Manager Confuses Default Error Message for "hack"](#)
[Ashlee Vance](#)
 - [The Spider of Doom](#)
[Alex Papadimoulis via Joe Loughry](#)
 - [The 2005 Helios B737 Crash - A test for Don Norman's Thesis?](#)
[Peter B. Ladkin](#) [Don Norman](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Motorist trapped in traffic circle for 14 hours**

<"Don Norman" <norman@nngroup.com>>

Sat, 1 Apr 2006 00:36:53 -0800

April 1. Hampstead, MA. Motorist Peter Newone said he felt as if a nightmare had just ended. Newone, 53, was driving his newly purchased luxury car when he entered the traffic circle in the city center around 9 AM yesterday, Friday. The car was equipped with the latest safety features, including a new feature called Lane Keeping. "It just wouldn't let me get out of the circle," said Newone. "I was in the inner-most lane, and every time I tried to get out, the steering wheel refused to budge and a voice kept saying over and over, 'warning, right lane is occupied.' I was there until 11 at night, when it finally let me out," Newone said from his hospital bed, his voice still shaky. "I managed to get out of the circle and to the side of the road, and then I don't remember what happened."

Police say they found Newone collapsed in his car, incoherent. He was taken

to the Memorial Hospital for observation and diagnosed with extreme shock and dehydration. He was released early this morning.

A representative of the automobile company said that they could not explain this behavior. "Our cars are very carefully tested," said Mr. Namron, "and this feature has been most thoroughly vetted by our technicians. It is an essential safety feature and it is designed so that it never exerts more than 80% of the torque required, so the driver can always overrule the system. We designed it that way as a safety precaution. We grieve for Mr. Newone, but we are asking our physicians to do their own evaluation of his condition."

Police say they have never heard of a similar situation. Mr. Newone evidently encountered a rare occurrence of continual traffic at that location: there was a special ceremony in the local school system which kept traffic high all day, and then there was an unusual combination of sports events, a football game, and then a late concert, so traffic was unusually heavy all day and evening. Attempts to get statements from relevant government officials were unsuccessful. The National Transportation Safety Board which is supposed to investigate all unusual automobile incidents says that this is not officially an accident, so it does not fit into their domain. Federal and state transportation officials were not available for comment.

✈️ Airbus A380 Evacuation Test

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>

Sat, 01 Apr 2006 00:02:41 +0200

Airbus has successfully completed the evacuation test on the A380, as reported in the news on 27 Mar 2006. 853 passengers were evacuated in less than the required 90 seconds from half of the exit doors, at the expense of minor injuries and one broken leg.

An Airbus spokesman said that the test had been successful: "In a group of 853 people, the chances that one person has a broken leg and doesn't yet know it are substantial. The test showed that everyone came out at least as healthy as when they went in."

Peter B. Ladkin, Causalis Limited and University of Bielefeld
www.causalis.com www.rvs.uni-bielefeld.de

✈️ Boeing B777 flight control anomalies

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>

Sat, 01 Apr 2006 00:01:11 +0200

I reported in [RISKS-24.03](#) ("Flight Control System Software Anomalies") on a partial-loss-of-control incident with a Boeing 777 aircraft that resulted in a US emergency Airworthiness Directive to replace the software in the air

data inertial reference unit (ADIRU) with an earlier version, while the manufacturer, Honeywell, developed a fix for the software.

It seems as if that is not the only problem at Honeywell. The *North German Herald-Advocate* reported on 28 Mar 2006 that the well-known Easter Egg writer and charter member of the International Aerobatic Club, Jody K. Beltramina, had retired from her position as Lead Avionics Software Developer in order to "spend more time with her family".

Peter B. Ladkin, Causalis Limited and University of Bielefeld
www.causalis.com www.rvs.uni-bielefeld.de

✶ Cartography dream realized

<"Don Norman" <norman@nngroup.com>>
Thu, 30 Mar 2006 01:56:27 -0800

Cambridge, UK. An old dream of cartographers has finally been realized through flat-panel displays and small, portable computational devices. For centuries, cartographers have dreamed of full-scale maps, that is, a map with a scale of 1:1, so that 1 Km. of the map would represent 1 Km. of the world. Implementation difficulties made such a map impractical. But now, scientists at Cambridge University have been able to display the full-scale map on a flat-panel screen, scrolling the map as necessary to cover the territory.

The new technique has already revealed important results: errors

in the existing geographical databases. These errors were revealed when geographers in Cambridge compared the full scale map with the terrain and discovered that they didn't fit precisely: Several structures, including a college building and several roads were determined to be in the incorrect location. "Rather interesting," said Lewis Carroll, spokesperson for the university, "several college buildings are quite off their correct location." Unfortunately, initial estimates for moving the buildings and roads to correct these discrepancies are too expensive, so, as Carroll puts it, "we will have to put up with these problems, but we will annotate the map to show where these placement errors occur."

An unexpected positive finding is that the map serves both types of map-users well: those who like to orient the maps so that North is always up, regardless of their direction of travel, and those who like to orient the map so that it corresponds to the positions of objects in the world. Now, either type of map user can be accommodated, something which was not possible when full-scale maps were implemented only on paper.

When asked what new developments might be expected from the college, Mr. Carroll stated that they were working on full-scale biographies, providing a much more realistic depiction of a person's life. This would allow a biography, for example, to take place in the same time-scale as the person's life, increasing the realism dramatically. Full scale renditions of other phenomena are in the works, but Carroll said that confidentiality

restrictions prevented discussion until they were fully realized.

✶ On the SAT errors (Epstein, [RISKS-24.21](#))

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

Sat, 1 Apr 2006 00:00:00 PST

The SAT service is reportedly contemplating the development of paperless Internet-accessible laptop-based SAT software that will in essence be like DRE voting machines, presumably with no audit trails and no ability to do rescoring apart from asking the SAT-taker to resubmit the answers! All students will most likely be required to use their own laptops or school-supplied systems, typically over unencrypted wireless and local networks. RISKS readers might also suspect that the SAT exam will be implemented as an unsigned ActiveX applet, and thus work only in IE. Perhaps other constraints as well will make students with Macs ineligible for college admission. This would be most unSATisfying. We hope the system will be more carefully designed and implemented, to level the playing field and to avoid numerous opportunities for cheating, collusion, and even malicious alterations of other students's exams. However, on the whole this item sounds too much like an April Fools' piece.

✶ Re: More SAT errors (Epstein, [RISKS-24.21](#))

<Richard Outerbridge <outer@sympatico.ca>>

Fri, 24 Mar 2006 20:58:23 -0500

OK, if these are the false NEGATIVES (scores less than deserved), how many false POSITIVES were there (scores more than deserved)?

And how many admission decisions were thereupon based?

[In reality, a bunch of overly high scores were reported, but those were apparently left unchanged. PGN]

✶ **Re: More SAT errors (Epstein, [RISKS-24.21](#))**

<Steve Schafer <steve@fenestra.com>>

Fri, 24 Mar 2006 00:10:00 -0500

I'm puzzled by the explanation put forth by Pearson regarding the cause of the October SAT mis-scoring (namely, humidity-induced dimensional changes in the test forms themselves). Everyone in the scanning business knows that the size of a piece of paper can vary substantially with the weather; that's why scannable test forms (e.g., Scantron) always include a number of registration marks around the edges of the page.

Could it be that the SAT forms don't contain a sufficient quantity and/or distribution of registration landmarks, or is the real problem somewhere else?

⚡ Man is charged \$4,334.33 for four burgers

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

Tue, 28 Mar 2006 16:24:28 PST

Do you believe in sanity clauses! Bounds checks?

An AP item datelined Palmdale, California notes that George Beane was charged \$4,334.33 for four burgers at Burger King. To make a long story short, the cashier entered \$4.33 and then forgetfully reentered the same amount again, resulting in a debit-card charge that instantly was paid out of his Bank of America account, wiping out their balance. After this was discovered, the bank insisted the funds were on a three-day hold and the debit could not be reversed. "For those three days, those were the most expensive value burgers in history," Pat Beane said.

http://hosted.ap.org/dynamic/stories/C/COSTLY_BURGERS?SITE=CAVAN&SECTION=HOME&TEMPLATE=DEFAULT

⚡ Offshore outsourcing cited in Florida data leak (Robert McMillan)

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

Mon, 27 Mar 2006 9:49:27 PST

Florida state employees who worked for the state during the 1.5 years beginning 1 Jan 2003 are being told that their personal information from the

state's People First payroll and human resources system may have been improperly transferred offshore by a subcontractor working for outsourcing service provider Convergys Corp. [Source: US laws may not help prevent PII disclosure, Robert McMillan, *ComputerWorld*; PGN-ed] <http://www.computerworld.com/securitytopics/security/story/0,10801,109938,00.html>

🔥 City Manager Confuses Default Error Message for "hack"

<Lizard <lizard@mrlizard.com>>

Mar 27, 2006 10:28 AM

http://www.theregister.co.uk/2006/03/24/tuttle_centos/

An Oklahoma town threatened to call in the FBI because its website was hacked by Linux maker Cent OS. However, it turns out CentOS didn't hack Tuttle's web site. The city's hosting provider had simply botched a web server. [Source: Oklahoma city threatens to call FBI over 'renegade' Linux maker: Our mistake is YOUR problem, Ashlee Vance, *The Register*, 24 Mar 2006; PGN-ed, from item on John McMullen's list, John F. McMullen, johnmac@acm.org johnmac@computer.org <http://johnmacrants.blogspot.com/> Lizard's blog: http://www.xanga.com/lizard_sf]

🔥 The Spider of Doom (Alex Papadimoulis)

<"Loughry, Joe" <joe.loughry@lmco.com>>

Wed, 29 Mar 2006 11:35:38 -0700

The Daily WTF: Curious Perversions in Information Technology,
Alex Papadimoulis, 28 Mar 2006

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

Josh Breckman worked for a company that landed a contract to develop a content management system for a fairly large government website. Much of the project involved developing a content management system so that employees would be able to build and maintain the ever-changing content for their site.

Because they already had an existing website with a lot of content, the customer wanted to take the opportunity to reorganize and upload all the content into the new site before it went live. As you might imagine, this was a fairly time consuming process. But after a few months, they had finally put all the content into the system and opened it up to the Internet.

Things went pretty well for a few days after going live. But, on day six, things went not-so-well: all of the content on the website had completely vanished and all pages led to the default "please enter content" page. Whoops.

Josh was called in to investigate and noticed that one particularly troublesome external IP had gone in and deleted **all** of the content on the system. The IP didn't belong to some overseas hacker bent on

destroying helpful government information. It resolved to googlebot.com, Google's very own web crawling spider. Whoops.

After quite a bit of research (and scrambling around to find a non-corrupt backup), Josh found the problem. A user copied and pasted some content from one page to another, including an "edit" hyperlink to edit the content on the page. Normally, this wouldn't be an issue, since an outside user would need to enter a name and password. But, the CMS authentication subsystem didn't take into account the sophisticated hacking techniques of Google's spider. Whoops.

As it turns out, Google's spider doesn't use cookies, which means that it can easily bypass a check for the "isLoggedIn" cookie to be "false". It also doesn't pay attention to Javascript, which would normally prompt and redirect users who are not logged on. It does, however, follow every hyperlink on every page it finds, including those with "Delete Page" in the title. Whoops.

After all was said and done, Josh was able to restore a fairly older version of the site from backups. He brought up the root cause -- that security could be beaten by disabling cookies and javascript -- but management didn't quite see what was wrong with that. Instead, they told the client to NEVER copy paste content from other pages.

✶ The 2005 Helios B737 Crash - A test for Don Norman's Thesis?

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>

Wed, 29 Mar 2006 10:53:48 +0200

PGN asked me some time ago (Oct 2005) about the Helios B737 aircraft accident in Aug 2005. I felt then that not enough was known, but that it likely had no connection with computers and little with digital automation. It is now pretty much known what happened, and certain features relate to the recent contribution by Don Norman in [Risks 24.17](#). Don said

"why not design things so that it [sic] can tolerate the well-known forms of human error? ... I have tried to deliver this message many times before. I predict that I will have to give it many times again."

and PGN suggested

"The RISKS archives themselves suggest that Don will have to continue this long-time consistent thread."

I think this accident provides a boundary case. An issue was raised in Nov 2005 about a possible crew confusion over the meaning of a warning tone. The same tone was used for an on-ground warning as well as an in-air warning, with different meanings. However, it is not at all clear that a different tone for each warning would have helped this crew. There are reported to be many other cases in which crews reacted appropriately, so this occurrence has precedents, all with a different outcome. The relevant

question is:

would one, as an engineer fully cognisant of Don's thesis, have designed these warnings differently? I incline towards the answer: no, this accident is an outlier. Others incline towards the answer yes. On with the story.

On 14 Aug 2005, a Helios Airways Boeing 737-300 on flight ZU 522 from Lanarca, Cyprus to Athens ran out of fuel and collided with terrain at Grammaticos, near Athens. The flight was scheduled to take about 1hr 20 minutes, and the aircraft had been airborne for nearly three hours.

The aircraft had been intercepted by Greek Air Force F-16s after being alerted by ATC. The interceptor pilots noted the copilot unconscious in his seat, and two other people on the flight deck, but not the captain. The cabin oxygen masks were deployed, but the copilot did not have his mask on (Flight International, 23-29 Aug 2005, p4, report by David Learmount).

The aircraft had been serviced before the flight; engineers carried out an on-ground pressurisation of the aircraft to see if the rear service door was leaking, because of a report that it was "noisy" on a previous flight. This check required the use, in manual mode, of the pressurisation control panel. The engineers opened the pressure relief valves after the successful check, to depressurise the aircraft. (Flight International, 13-19 Sep 2005, p15, report by David Learmount).

Normal flight crew pre-take-off procedures would have them

select cabin altitude to 8,000 ft and the pressurisation switch to automatic (ibid. 13-19 Sep 2005).

The cabin altitude (CA) warning horn activated as the aircraft passed through 14,000 ft out of Lanarca in climb to its cruising altitude of 34,000 ft, and it was not canceled for the rest of the flight. The captain called the Helios engineering department on the company frequency. Another alert had sounded just after the CA warning had activated, warning that the avionics bay cooling fans were not operating. Helios's engineering department said that the captain's request was unclear. They asked him whether the pressurisation panel had been reset to automatic from manual. He responded by asking where the circuit breaker was for the avionics bay fans. Engineering told him it was behind his seat. That was the last communication of any sort from the aircraft. There is no recording of this conversation; the report comes from the former Helios chief engineer. (ibid., 13-19 Sep 2005).

The aircraft manufacturer Boeing issued a "multi-operator message" to B737 users in Sep 2005 to remind them that both the CA warning and takeoff configuration warning horn are the same sound; that the takeoff configuration warning can sound only when the aircraft's weight is on the wheels; and that if the same alert sounds in flight, it is the CA warning.

The chief investigator told David Learmount at a safety seminar in Moscow in

Nov 2005 that the pressurisation was set to manual, so that the aircraft did not pressurise as it climbed, and the crew failed to notice this in pre-take-off checks; the crew thought the CA warning was an erroneous takeoff configuration warning, and their "subsequent mindset and actions were determined by this preconception until hypoxia overcame them as the aircraft continued to climb." (Flight International, 15-21 Nov 2005, p9, report by David Learmount).

I used to climb up mountains, and have been at altitude without oxygen in small aircraft. The symptoms and dangers of hypoxia should be known to practitioners of both activities. Indeed, I get hypoxic when doing interval training on my sport bicycle mounted on the home trainer. It is insidious, in that gradually reducing ability to concentrate is accompanied by lowered self-awareness and feelings of well-being - before, if it does too far, one loses consciousness. But I had thought that any reasonably aware and well-trained pilot would know how to recognise the symptoms before it got to that stage. When I flew high, I used to write my signature regularly on my kneeboard, the idea being that when it got hard, or the signature too straggly, it was time for an immediate descent. I found that this view did not resonate with many pilot colleagues. I talked about it in Oct 2005 to a colleague who is a senior aviation accident investigator and human factors specialist at one of the most respected accident investigation organisations. He pointed out that in the situations in which I had

experienced hypoxia, I could have expected it and therefore was particularly attuned to the symptoms. Also that I seemed to have had known and varied experience with it and through this experience was likely more cognisant of the symptoms as they start to occur. He suggested that one could not necessarily expect a flight crew with no altitude-chamber or other experience to recognise hypoxia and get their masks on before passing out. So it seems that my puzzlement over why the crew had not recognised their hypoxia was misplaced.

It remains, though, that the CA warning sounded as it should, and the flight crew did not react appropriately. Why not?

There have been "many other cases of a Boeing 737 aircraft climbing without pressurisation set, but the crews recognised the alerts and averted crew hypoxia and resultant disaster" (ibid., 15-21 Nov 2005).

A report in a German newspaper said that Greek television on 19 Sep 2005 had reported that the coroner had said that the captain had 45% blockage of the coronary arteries and the co-pilot had 90% blockage of the coronary arteries (*Die Welt*, 20 Sep 2005). That would render them particularly susceptible to quick onset of hypoxia and resulting unconsciousness.

Fact remains that, under the influence of hypoxia, the crew appeared to be confused over the meaning of the CA alert.

On the one hand, the warning is identical to that of the takeoff configuration warning. On the other hand, these are professional pilots who

are required to know the meaning of the alerts that activate in their aircraft. This alert is unambiguous: on the ground, it is the takeoff configuration warning. In the air, it is the CA. And "many" other crews have experienced the same sequence of warnings and reacted appropriately.

There were apparently serious communication problems within the crew and between crew and their engineering departments. Both the German captain and the Cypriot co-pilot had trouble with English (the engineers were British and had trouble communicating with them about the problems); but that was also the only language which they had in common.

The chief investigator, Capt. Akrivos Tsolakakis, addressed the European Aviation Safety Seminar in Athens in March 2005, and said that "latent errors have lain there for years waiting for the pilot to pull the trigger". He said that all the parties involved contributed to the systemic latent faults that led to the accident He did not specify the faults or the responsibilities. The draft report has been prepared; involved parties have 60 days to comment and the final report is likely to be ready for publication in June or July 2006 (Flight International, 21-27 March 2006, report by David Learmount).

It seems as if we will read a Reason-type "Swiss Cheese" explanation of the accident; the vocabulary stems from e.g., his influential book Human Error (Cambridge U.P., 1990).

One might speculate that, had the CA warning had a unique sound,

the crew could have recognised it for what it is, rather than confusing it with another alert. If this speculation were to be correct, the Counterfactual Test would lead us to conclude that the CA warning/takeoff configuration warning doublet was a causal factor in the accident. On the other hand, the crew did not seem to know what it meant in any case; their engineering department did know, but engineering's attempts to alert them directly to possible pressurisation problems failed. A different sound does not help any if one doesn't know what it means and cannot follow the appropriate advice of those who do.

I doubt whether the final report will be able to give us much guidance on which of these positions it is more reasonable to accept.

Peter B. Ladkin, Causalis Limited and University of Bielefeld
www.causalis.com www.rvs.uni-bielefeld.de

✶ The 2005 Helios B737 Crash - A test for Don Norman's Thesis?

<"Don Norman" <don@jnd.org>>
Wed, 29 Mar 2006 05:03:42 -0800

Peter Ladkin properly points out that the Helios 737 accident in 2005 is complex, and so it can be attributed to multiple causes. But I happen to be a fan both of Swiss Cheese and of Jim Reason: Reason and I have worked on error theory together.

I agree that the circumstances described -- crew hypoxia -- makes it impossible to know how much the modal characteristic of the warning signal contributed to the accident. Nonetheless, I contend that modes in general are a bad idea and are well-known sources of difficulty, whether they be in computers, industrial controls, or as in this case, the meaning of a particular warning signal. When something is modal, then its interpretation depends upon the system state, which adds to the mental workload and has been a known source of difficulty in many situations. With the case of a crew with diminished mental capacities (because of hypoxia), I suspect that the extra workload required to interpret the modal warning signal increases the likelihood of a misinterpretation. Of course, in this particular case, the crew may already have been so impaired that nothing would have helped.

We will never know. Errors by highly trained pilots are rare, and so difficult to study. Ladkin points out that other crews have properly interpreted the signal. But those crews were not suffering from hypoxia to a similar extent (although we don't really know for sure). And in any event, with low-probability events, a few successes does not mean that the system is trustworthy. (I suspect we are in agreement on this point.)

But why take the chance? There is no harm in ensuring that all safety-critical warning signals be unique and distinct (that is, modeless).

There may be no benefit either, but any cost analysis comes out in favor of

eliminating modes: Minimal cost to do so, possible huge loss if one does not.

But thanks to Peter Ladkin for once again providing us with a detailed analysis of the many factors that go into accidents in commercial aviation. Aviation today is so safe, that we have few accidents to investigate, and each of these is always complex, filled with mitigating and possibly causal sequences. Any simple interpretation of such an accident is bound to be wrong.

Don Norman, Nielsen Norman Group and Northwestern University
<http://www.jnd.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

Search RISKS using [swish-e](#)

Volume 24: Issue 23

Tuesday 4 April 2006

Contents

- [Three days of San Francisco BART upgrade crashes](#)
[PGN](#)
- [Nashville airport X-ray baggage screeners offline: "software glitch"](#)
[Carl G. Alphonse](#)
- [IT Corruption in the UK](#)
[Jerome Ravetz](#)
- ["Invisible fences" pose risks for dogs from coyotes](#)
[Philipp Hanes](#)
- [Computer problems with voting system](#)
[Danya Hooker via Dana A. Freiburger](#)
- [eFax/J2 opens door to expensive Joe-jobbing](#)
[Dallman Ross](#)
- [Fake E-Mail Topples Japan Opposition Party](#)
[Hans Greimel excerpt](#)
- [phishing@irs.gov](#)
[Al Macintyre](#)
- [Maplin gives "How To..." advice on Wireless Networks](#)
[Chris Leeson](#)

- [Rootkit: erosion of terms?](#)
[Rob Slade](#)
 - [Error bounds on estimated probabilities](#)
[Jacob Palme](#)
 - [Re: Excel garbles microarray experiment data](#)
[Przemek Klosowski](#)
 - [Re: It's now a crime to delete files](#)
[Crispin Cowan](#)
 - [Re: The Spider of Doom](#)
[Steve Summit](#)
 - [Re: The 2005 Helios B737 Crash - A test for Don Norman...](#)
[Martyn Thomas](#) [Tom Watson](#) [noone](#) [Eric T. Ferguson](#)
 - [Re: Man is charged \\$4,334.33 for four burgers](#)
[Mark Feit](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Three days of San Francisco BART upgrade crashes

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

Fri, 31 Mar 2006 07:12:11 PST

BART has been attempting a software upgrade to modernize the software controlling its rapid transit system. Unfortunately, computer system problems were responsible for a combination of system-wide slowdowns and shutdowns on three consecutive days (Monday/Tuesday/Wednesday), including during rush hours. The first two days' problems resulted from observed potential safety failures of the new software. The third day's problems resulted from an attempt to revert to a backup system -- which apparently overloaded a network switch, which crashed the computer system. The new

supposedly self-correcting software had passed all of its tests on the previous Sunday, but evidently the testing was incomplete. (This upgrade is only part of what is thought to be a carefully phased multiyear modernization that is expected to take at least another five months.)

[Sources: PGN-ed from an item in the *San Francisco Chronicle*, 30 Mar 2006, the *San Jose Mercury*, 30 Mar 2006 <http://www.mercurynews.com/mld/mercurynews/14223072.htm> and Computerworld, 31 Mar 2006.]

✈ Nashville airport X-ray baggage screeners offline: "software glitch"

<"Carl G. Alphonc" <alphonc@cse.Buffalo.EDU>>
Fri, 31 Mar 2006 21:22:23 -0500

As reported at www.cnn.com/2006/TRAVEL/03/31/airport.security.ap/index.html:

A software glitch knocked out the computerized X-ray machines at Nashville International Airport for five hours Friday, causing long lines and flight delays.

No indication of what the glitch might be. The article goes on to state:

David Beecroft, who oversees security operations at Nashville for the federal Transportation Security Administration, said all U.S. international airports were alerted because the company that supplies the software for the Smiths Heimann X-ray detectors also serves several

other airports. But TSA spokeswoman Laura Uselding later said other airports were not notified because the situation in Nashville was an isolated event. The discrepancy could not be immediately resolved.

There are two discrepancies as I see it. Was this an isolated event or one that affected screening machines at several airports? Were several airports alerted or not?

Also some questions come to mind. If there was a problem, why would only *international* airports be alerted (shouldn't domestic baggage be screened with correctly functioning equipment)? Were these machines perhaps only used at intl airports (this isn't clear from the story)?

Carl Alphonse, Dept of Computer Science and Engineering,
University at Buffalo
Buffalo, NY 14260-2000 www.cse.buffalo.edu/faculty/alphonse 716-645-3180 x115

✈ IT Corruption in the UK

<Jerome Ravetz <jerome-ravetz@tiscali.co.uk>>

Sun, 2 Apr 2006 11:59:43 +0100

The 2 Apr 2006 issue of the Sunday Times has an article by the distinguished journalist Simon Jenkins, 'Desperate Dispatches from the banana republic of Great Britain'. There he lists a number of multi-million pound scams. I have told him by way of consolation that in the U.S.A. they multi-billions.

Here was one item that he missed!

In a recent **Private Eye** (#1154, 17 March 2005, p.4) we have the following item, starting:

`How appropriate that Mapeley, the company that does most of its business through secretive tax havens -- hotbeds of money laundering, terrorist financing and tax dodging -- should win the contract to manage the 70-odd 'authentication by interview' centres at which the Passport Service will vet and biometrically test new applicants in the interests of national security.'

The Eye goes on to remind readers of Mapeley's questionable record as financial manipulators. For readers of RISKS, it is more interesting that the UK government has chosen this firm -- which at best has no experience whatever in the field -- to manage the introduction of a controversial, untried, rapidly developing and highly sensitive technology. In that anyone with the most elementary prudence would recognise that the ID card scheme will immediately attract hackers, criminals and terrorists to come in on the ground floor, this contract is evidence for the genuineness of the Blair government's commitment to security.

Jerry Ravetz, 111 Victoria Road, Oxford OX2 7QG James Martin
Institute for
Science and Civilization, Oxford www.jerryravetz.co.uk +44 [0]
1865 512247

✦ "Invisible fences" pose risks for dogs from coyotes

<"Philipp Hanes" <philippphanes@hotmail.com>>

Tue, 04 Apr 2006 17:03:50 +0000

The cited article concerns dogs that are given electrically activated collars to keep them in their virtually enclosed yards. Unfortunately, coyotes -- who obviously don't have the collars -- can easily enter the dogs' yards, and have been reportedly killing dogs. [PGN-ed; This situation is another variant on attempting to solve one problem without considering others, in this case considering the confinement problem without remembering the intrusion problem, which is sometimes seen in simple-minded computer security approaches -- as is its converse.]
<http://www.pioneerlocal.com/cgi-bin/ppo-story/localnews/current/gl/03-30-06-876429.html>

[Moral: Bilateral perimeter (de)fences are more effective than border collars for border collies? PGN]

✦ Computer problems with voting system (Danya Hooker)

<"Dana A. Freiburger" <dafreiburger@wisc.edu>>

Fri, 31 Mar 2006 07:09:52 -0600

Computer problems caused the University of Wisconsin-Madison Student Council to throw out online votes cast this week for campus offices, but retained

votes cast for two referendums on the same ballot. The cause of the problem may have been a "little-used, multiple-name tool has worked in prior elections but may have been corrupted by a database upgrade several months ago." The main risk appears to be the lack of testing of the voting system prior to the vote (along with no testing after a major software upgrade).

The parallels with the world of voting machines are obvious: the voting system needs to be tested and certified BEFORE voting occurs.

Six thousand votes for Student Council seats will be tossed out, but votes cast for two referendums will be counted, under a plan approved by the Associated Students of Madison on Wednesday night. [...] [Source: Students plan to toss council votes after glitch Danya Hooker, dhooker@madison.com, *Wisconsin State Journal*, 31 Mar 2006] <http://www.madison.com/wsj/home/local/index.php?ntid=78393>

eFax/J2 opens door to expensive Joe-jobbing

<"Dallman Ross" <dman@spamless.us>>
Thu, 30 Mar 2006 02:24:02 +0200

eFax, which is owned by j2.com (a.k.a. "jFax"), recently sent me a member e-mail containing the following text:

```
> eFax Tip for Easier Faxing
> How to send a fax by e-mail
> 1. Open a new e-mail.
> 2. Add fax number (including country code) to
> "@efaxsend.com".
```

- > 3. Attach the document you wish to fax.
- > (supported file types
- > <http://mx3.efax.com/redir3/zYEGTw_CD!https://www.efax.com/en/efax/twa/page/supportedFileTypesPopup>)
- > 4. Send e-mail. We'll convert the attachment and fax it for you.
- >
- > You'll receive a confirmation e-mail once the fax has been delivered.
- >
- > Example
- > 1. You want to send a fax to London (UK's country code: 44)
- > 2. Fax number is (0) 20 7555 1234
- > 3. You would type: 442075551234@efaxsend.com

Sounds neat, you say? I thought so too, for a second or two. Then it dawned on me: how will they know whom to bill?

The answer seems to be that they bill member accounts based simply on the From-address! That is, if Mr. Joe-Jobber with a nit to pick against you knows that you have an eFax or j2 account and knows or guesses the e-mail address you use with that service, he can send a spate of bogus (or real) faxes using your address and clear your account or bank balance!

One acquaintance of mine tested this with his j2 account. No prior registration for this service was required. He simply e-mailed as above, and his account was debited 10 cents and the fax was sent.

There does not seem to be any way to disable e-mail addresses from this service, for anyone with an eFax or j2 account. One can, of course, change the registered e-mail address used with the service, however.

What an accident waiting to happen this is, all in the name of "convenience"!

Dallman Ross <http://vsnag.spamless.us/> - plug-in for procmail

⚡ Fake E-Mail Topples Japan Opposition Party

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

Sun, 2 Apr 2006 12:02:49 PDT

Japan's opposition party suffered a fresh humiliation Friday when its leadership resigned en masse over a fake e-mail scandal, handing Prime Minister Junichiro Koizumi an uncontested grip on power in his last six months in office. ... Party leader Seiji Maehara and his lieutenants stepped down after the party's credibility was torpedoed by one of its own lawmakers, who used a fraudulent e-mail in an apparent attempt to discredit Koizumi's ruling Liberal Democratic Party. [Source: Hans Greimel, Associated Press, 31 Mar 2006; PGN-excerpted. TNX to Lauren Weinstein for noting this one.]
<http://www.newsday.com/news/nationworld/wire/sns-ap-japan-politics,0,191417.story?coll=sns-ap-nationworld-headlines>

⚡ phishing@irs.gov

<Al Macintyre <macwheel99@sigeom.net>>

Tue, 28 Mar 2006 01:30:24 -0600

phishing@irs.gov is an e-mail address with the IRS where we can

forward

e-mails that we think fraudulently claim to come from the IRS.

Example

scams include: claim that a tax refund is owed you

<http://www.fcw.com/article92749-03-27-06-Web>

<http://en.wikipedia.org/wiki/User:AlMac> <http://www.ryze.com/go/>

[Al9Mac](#)

Maplin gives "How To..." advice on Wireless Networks

<"LEESON, Chris" <chris.leeson@atosorigin.com>>

Mon, 3 Apr 2006 14:20:04 +0100

I dropped in to one of my local Maplin (www.maplin.co.uk) stores today.

While standing in the queue, I noticed a leaflet entitled "How to...Create a wireless network".

It was full of useful information (the 5 most important advantages of a wireless network are, apparently, no messy cables; no need to drill holes; simple to expand for more users; the ultimate freedom - Internet anywhere in your house of garden; no need to open up your PC to install hardware).

Alas, absolutely nothing about the risks of a wireless network, and nothing on how to secure one. Bear in mind that this is supposedly a "how to...", not an advert.

They did, however, offer a link (www.maplin.co.uk/wireless) with more information. When I got back to the office I tried the link,

hoping for a more complete set of instructions dealing with the issues - after all, there is a limit to what can be put on an A4 sheet.

The further information consisted of the phrase "DETAILS TO FOLLOW...". I waited for a few minutes just in case there was a flash animation loading or a page redirect being especially slow. Then I checked the page source. No flash, no redirect - they just hadn't uploaded the page.

Risks?

1. Pushing technology without due regard to security (a common topic in RISKS, alas).
2. Publishing literature with web links in. but not having them ready when the literature is released, does not reflect well on a company.

⚡ Rootkit: erosion of terms?

<Rob Slade <rMslade@shaw.ca>>
Tue, 04 Apr 2006 12:57:53 -0800

Wearing my "glossary guy" hat, one of the things I've noticed is how difficult it is to come to complete agreement on the precise definition of many terms that are used in infosec. There are, for example, three quite distinct meanings for the term "tar pit." (And that's in terms of networking alone.) (It is highly unlikely that we will ever be able to reduce the number of tar pit definitions to one: all the

definitions came at
about the same time, and all are important and equally valid.)

However, what really irks me is when defined and agreed upon
terms start
being misused, sometimes to the point where the original term
becomes
useless. There is, of course, "hacker." (And I've given Hal a
diatribe
about "zero day" which will probably be coming out in the next
ISMH.)

The latest endangered term seems to be "rootkit." A rootkit has
been
defined as programming that allows escalation of privilege or
the option to
re-enter the compromised system with greater ease in the
future. Often
rootkits also contain functions that prevent detection of, or
recovery from,
the compromise.

Starting with the recent Sony "digital rights management"
debacle, the
general media now seems to be using "rootkit" to refer to any
programming
that hides any form of information on a system, and specifically
any
functions that impede the detection of malware. The latest
reports are that
Bagle and other malware/virus families now contain "rootkits."
Antidetection features in viruses are nothing new: there was a
form of
tunneling stealth implemented in the Brain virus 20 years ago.
Therefore,
to use the term rootkit to refer to this activity can only
degrade the value
of the term.

It has been difficult to ensure that infosec specialists can at
least talk
to each other and exchange useful information. However, this
may not last

much longer if our "precious verbal essences" become contaminated.

rslade@vcn.bc.ca
niu.edu

slade@victoria.tc.ca

rslade@sun.soci.

✉ Error bounds on estimated probabilities

<Jacob Palme <jpalme@dsv.su.se>>

Sun, 2 Apr 2006 11:17:40 +0200

Martyn Thomas ([RISKS-24.19](#)) asks about the use of error bounds on estimated probabilities.

There is actually one researcher, Love Ekenberg, who has built a theory of error bounds on probability estimates, and also developed software to help in evaluating different alternatives where such error bounds are used.

His software is described at

http://www.preference.nu/site_en/index.php

Jacob Palme <jpalme@dsv.su.se> (Stockholm University and KTH)

URL: <http://www.dsv.su.se/jpalme/>

✉ Re: Excel garbles microarray experiment data (Malcolm, [RISKS-24.21](#))

<Przemek Klosowski <przemek@gwyn.tux.org>>

Fri, 24 Mar 2006 22:57:58 -0500

While working on a joint UK / German product development we discovered

that the 'standard' separator employed in many German CSV files is the

semi-colon ';' - I do not know why.

Probably because Germans use 'decimal comma' instead of 'decimal point' between the integer and fractional parts of a floating point

number, thus interfering with the use of comma in CSV files. The period is used for grouping of digits, i.e. every three digits.

[Also noted by George M. Sigut. This is a very old problem that has

been noted in RISKS on numerous occasions. It keeps recurring. PGN]

✶ **Re: It's now a crime to delete files (Peterson, [RISKS-24.20](#))**

<Crispin Cowan <crispin@crispincowan.com>>

Wed, 29 Mar 2006 11:47:19 -0800

> The 7th Circuit made two remarkable leaps. First, the judges said that
> deleting files from a laptop counts as ``damage''. Second, they ruled that
> Citrin's implicit ``authorization'' evaporated when he (again, allegedly)
> chose to go into business for himself and violate his employment contract.

This actually makes perfect sense to me, on both counts. File deletion is damage, and both the laptop and the data seem to have been the property of IAC at the time that he chose to destroy the data.

Imagine sacking a developer, and the developer deletes all the source code he has written during his employment before leaving the building. Such data vandalism is justifiable only if you also plan to return all wages paid during employment, and even then the employer should have the choice.

More over, depending on the terms of the employment contract, Citrin may not even have had a right to a copy of the data for himself.

Crispin Cowan, Ph.D. <http://crispincowan.com/~crispin/>

⚡ Re: The Spider of Doom ([RISKS 24.22](#))

<Steve Summit <scs@eskimo.com>>

Sat, 01 Apr 2006 17:24:22 -0500

"one particularly troublesome external IP had gone in and deleted **all** of the content on the system [...] googlebot.com, Google's very own web crawling spider. ... the CMS authentication subsystem didn't take into account the sophisticated hacking techniques of Google's spider."

I can see Joe Loughry's tongue in his cheek pretty clearly from here, but it might not be obvious to a casual reader that this was manifestly **not** a "hacking" attempt by Google. That a simple and naive traversal of some hyperlinks could cause content to be deleted makes it pretty obvious that something was badly wrong with the site's editing and access-

control model.

Needless to say (or, it *ought* to be needless, but is actually pretty needful), security that assumes that visitors *will* have cookies and JavaScript enabled, that can be compromised if these features are disabled, is no security at all. That content could have been inadvertently deleted by any visitor to the vulnerable website; google's spider just happened to get to it all first.

✉ RE: The 2005 Helios B737 Crash ... ([RISKS-24.22](#))

<"Martyn Thomas" <martyn@thomas-associates.co.uk>>

Sat, 1 Apr 2006 15:25:08 +0100

Why is it necessary for the cabin pressurisation switch to have the property that it is possible to leave it set to manual, accidentally, on takeoff?

Wouldn't a thorough hazard analysis reveal the risk, and normal systems engineering (reducing risk ALARP) eliminate it?

Surely it would be safer if all settings defaulted to normal on start-up, and required explicit setting to hazardous positions. Are there other such known traps on commercial aircraft?

✉ Re: The 2005 Helios B737 Crash - A test for Don Norman... (R-24:22)

<"Tom Watson" <t_wtom@qualcomm.com>>

Mon, 3 Apr 2006 14:42:26 -0700

While we all speculate on the cause of the error, if the pilots were in communication with the engineering department of the airline, it seems that the ground people might want to say to the flight deck crew something like "Oxygen Now!!" then diagnose the problem. If the flight deck people had oxygen (they were by recollection communicating with the ground people), this might have brought them to their senses so they could solve the problem.

I guess it stems from the "If you are up to your ass in Alligators, you forget that the original objective was to drain the swamp!" syndrome. Sometimes you drain the swamp before dispatching the alligators, and suffer the consequences. -- Tom Watson Generic Signature
t_wtom@qualcomm.com (I'm at work now)

✶ The 2005 Helios B737 Crash (Re: [RISKS-24.22](#))

<noone <noone@mtechnology.net>>

Mon, 03 Apr 2006 15:53:03 -0400

One aspect of the Helios B737 crash not discussed by either Peter Ladkin or Don Norman ([RISKS-24.22](#)) is the relatively short interval available for

the crew to discern the problem and take corrective action.

According to a published accident report (<http://aviation-safety.net/database/record.php?id=20050814-0>) the airplane climbed from Larnaca airport, at sea level, to 34,000 feet in approximately 19 minutes. That means an average rate of climb of nearly 1,800 feet per minute (FPM). Normally jets climb rapidly from takeoff to 10,000 feet in order maintain a speed of 250 knots or less, then enter a cruise climb with higher airspeed and better fuel economy, although air traffic control can require deviations. I was unable to find any more detailed information about the climb profile of this particular flight.

From the time the cabin altitude alert went off at 12,000 feet (http://www.nts.gov/nts/brief2.asp?ev_id=20050825X01309&ntsno=DCA05RA092&akey=1) it would take just 6 minutes and 40 seconds to reach 24,000 feet if the climb rate was 1,800 FPM.

The Time of Useful Consciousness (TUC) at 24,000 feet is at most 3 minutes (<http://www.smartcockpit.com/operations/Surviving%20Cabin%20Decompression.pdf>, http://www.aviationmedicine.co.za/AM_S_Hypoxia.php). Victims of hypoxia may be conscious after the TUC but are incapable of taking proper corrective and protective action, even when instructed or coached. The TUC is further reduced by the rate of change of altitude, by increased mental activity, such as pilot workload in an emergency, and by exercise, such as struggling out of a cramped cockpit seat to check circuit breakers.

Apparently the captain and co-pilot did not don their oxygen masks when the cabin altitude alarm sounded. The "Surviving Cabin Decompression" document discusses incidents where pilots alerted by an explosive or rapid decompression lost consciousness after brief delays in donning their masks. These events are announced by unmistakable cues such as a loud bang and/or mist forming in the cabin.

The slower loss of pressure as the accident airplane climbed appears to have allowed hypoxia to develop without these cues. It would probably take a few minutes after an initial radio call to base to get qualified engineering assistance to the microphone. The fact that neither flight crew member responded to the Helios engineering department instruction/question regarding the status of the pressurization panel indicates that hypoxia was probably far advanced by the time the instruction was given.

In the US, Federal Aviation Regulations require that whenever the airplane is above 25,000 feet, if one pilot leaves the controls, the other must don an oxygen mask. The rules may be different in Greek airspace. There are reports (e.g., <http://www.airlinesafety.com/editorials/737CrashInGreece.htm>) that this regulation is not always strictly observed.

Had the Helios co-pilot followed this rule when the captain left his seat, this accident would have been prevented, regardless of the crew's apparent misunderstanding of the cabin altitude alarm. Even if he was so trained, his hypoxia may have prevented him from performing normally.

Most depressurization incidents are resolved without fatal crashes. This and other depressurization accidents demonstrate how little time is available for even fully trained, alert, and competent flight crew to don their oxygen masks and prevent a tragedy. The uniqueness of the warning signal may or may not have played a role in this case; the short interval between the first indication of trouble and complete incapacitation of the crew certainly did so.

✈️ **Re: Helios B737 Crash ([RISKS-24.22](#))**

<"Eric Ferguson" <e.ferguson@antenna.nl>>

Sun, 02 Apr 2006 09:42:11 +0200

I am astonished at the underlying safety concept.

It is obvious that climbing with no pressurization and no (crew and passenger) oxygen is fatal. Then why just issue a "warning"?

I would propose this Basic safety concept: before the system will allow itself to move into dangerous situations, the pilot must confirm that he is aware of the specific danger involved.

Implementation for this case: well before attaining a dangerously low cabin pressure, the autopilot refuses to allow further climbing (even manual) until the pilots override this barrier by confirming explicitly "we have donned oxygen".

The same system would - in case of high altitude depressurization -- initiate an automatic rapid descent until the pilots override it with the same confirmation.

Dr.ir. Eric T. Ferguson, Consultant for Energy and Development,
van Reenenweg 3, 3702 SB ZEIST Netherlands +31 30-2673638 e.
ferguson@antenna.nl

✈ Re: Man is charged \$4,334.33 for four burgers ([RISKS-24.23](#))

<Mark Feit <mfeit@notonthe.net>>

Sat, 1 Apr 2006 09:13:00 -0500

Credit cards are relatively new things for fast food restaurants. Just about every one I've set foot in recently hasn't upgraded its point-of-sale systems to integrate them beyond adding a "paid by credit" button so there won't be cash expected in the till. Card transactions are being handled separately by VeriFone or similar countertop terminals which have no idea whether you're selling French fries or Ferraris.

Transactions at countertop terminals do have a bounds check, but it happens at the wrong point in the transaction. The customer receipt and store copy are printed *after* the charge has been committed to the clearing house, leaving the cardholder with no way to approve the amount. (Even restaurants, which have an extra step where you add a gratuity, have this problem, because the final figure is still un-verified by the

customer.)

Even if the customer refuses to consummate the transaction by signing, it's still a done deal and the only recourse for correcting it is to take it up with the bank.

I suspect that's what happened in this case, and it's a very good reason to use a real credit card instead of a debit card.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 24

Wednesday 12 April 2006

Contents

- [Casino can reprogram slot machines in seconds](#)
[PGN](#)
- [Deleting May Be Easy, but Your Hard Drive Still Tells All](#)
[Eric Taub via Monty Solomon](#)
- [Man Gets \\$218 Trillion Phone Bill](#)
[Les Hatton](#)
- [Borders with Customs computers](#)
[David Magda](#)
- [Australian police inadvertently reveal e-mail addresses/passwords](#)
[Mike Martin](#)
- [The risks of scaling incompetence to big numbers](#)
[Poul-Henning Kamp](#)
- [Secure colocation in the North Sea](#)
[Dan Jacobson](#)
- [Classified military documents exposed through file sharing](#)
[Diomidis Spinellis](#)
- [Unexpected Internet Explorer behaviour when copy/pasting](#)
[Pierre Pierre Blais](#)

- [Re: Three days of San Francisco BART upgrade crashes](#)
[Martyn Thomas](#)
 - [Re: Rootkit: erosion of terms?](#)
[Steven M. Bellovin](#)
 - [Washington voting hijacked by computer mischief](#)
[Peter Gregory](#)
 - [Computer problems with U.Wisconsin voting system](#)
[Dana A. Freiburger](#)
 - [Risks of email-to-fax services](#)
[Jim Youll](#)
 - [Re: Man is charged \\$4,334.33 for four burgers](#)
[Martin Ward](#)
 - [Helios B737 Crash](#)
[Michael Loftis](#) [David Alexander](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Casino can reprogram slot machines in seconds

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

Wed, 12 Apr 2006 11:10:27 PDT

As an enormous operational improvement, the 1,790 slot machines in Las Vegas's Treasure Island Casino can now be reprogrammed in about 20 seconds from the back-office computer. Previously this was an expensive manual operation that required replacing the chip and the glass display in each machine. Now it is even possible to have different displays for different customers, e.g., changing between "older players and regulars" during the day and a different crowd at night ("younger tourists and people with bigger budgets". (Slot machines generate more than \$7B revenue annually in

Nevada.) Casinos are also experimenting with chips having digital tags that can be used to profile bettors, and wireless devices that would enable players to gamble while gamboling (e.g., in swimming pools!). [Source: Article by Matt Richtel, Prefer Oranges to Cherries? Done! *The New York Times*, 12 Apr 2006, C1,C4; PGN-ed]

There are various risks of interest to RISKS. Regulators are concerned that machines might be "invaded by outsiders", while bettors are concerned that casinos could be intentionally manipulating the odds -- for example, giving preferential treatment to high rollers. Internal and external manipulation are clearly potential issues, which of course could be exacerbated by compromisable wireless security. By Nevada law, odds cannot be manipulated while someone is playing, although with four-minute timeouts before and afterward, machines may be reprogrammed on the fly.

If it were still April Fools' Day, I might suggest that the slot machines could be reprogrammable for use as voting machines on election day. That way you could have instant payoff if you vote the right way.

⚡ Deleting May Be Easy, but Your Hard Drive Still Tells All (Taub)

<Monty Solomon <monty@roscom.com>>
Mon, 10 Apr 2006 08:55:00 -0500

Scott Cooper, a computer forensics expert, discovered that a "1" digit had

been deleted from a 20-page digital contract in Microsoft Word. His work discovered when the document had been changed and by whom, and resulted in his client receiving the originally contracted 15% share instead of the altered 5% share in his sold company, that is \$96M instead of \$32M.

[Source: Eric A. Taub, *The New York Times*, 5 Apr 2006; PGN-ed]
<http://www.nytimes.com/2006/04/05/technology/techspecial4/05forensic.html>

🔥 Man Gets \$218 Trillion Phone Bill

<Les Hatton <L.Hatton@kingston.ac.uk>>
Wed, 12 Apr 2006 16:25:07 +0000

A Malaysian man said he nearly fainted when he received a \$218 trillion phone bill and was ordered to pay up within 10 days or face prosecution.

Yahaya Wahab said he disconnected his late father's phone line in January after he died and settled the 84 ringgit (\$23) bill, the *New Straits Times* reported. But Telekom Malaysia later sent him a 806,400,000,000,000.01 ringgit (\$218 trillion) bill for recent telephone calls ... [more].

[Source: Associated Press, 10 Apr 2006]

An interesting one this. Unless this got misprinted somewhere, they must have gone to 64-bit arithmetic to issue bills this big. If they have implemented it as fixed point arithmetic and sucked up about 7 bits for the fraction, that would leave about 56 bits in signed

arithmetic to play

with which according to my trusty Linux version of bc would allow them to

issue a bill up to:-

72,057,594,037,927,936 ringgits. or around \$2 quadrillion.

Of course they could have gone to arbitrary precision arithmetic in the

hope of making a fast googleplex or two.

The guy is actually lucky because at least its obviously stupid. It could

have equally well been an erroneous number which was vaguely reasonable

but expensive and because the computer says it, it must as we all know, be

right.

✶ Borders with Customs computers

<David Magda <dmagda@ee.ryerson.ca>>

Wed, 12 Apr 2006 08:02:27 -0400

In August 2005, the computer systems used by US Customs failed for about

five hours ([RISKS-24.02](#)).

Documents obtained through a freedom of information request by *WiReD*

actually point to a virus being the culprit. The main issue being that a

security patch was not deployed (on purpose), but once the virus threat was

found, the patch was pushed out to the systems.

One sentence in the story [1] jumped out at me, though:

> Publicly, officials initially attributed the failure to a virus, but later
> reversed themselves and claimed the incident was a routine system failure.

I'm curious to know why "system failure" is considered "routine". While it is prudent to plan for things breaking (redundancy, backups, etc.), and it will inevitably happen in many cases (especially in physical systems), should it ever be considered "routine"?

[1] <http://www.wired.com/news/technology/0,70642-0.html>

✶ Australian police inadvertently reveal e-mail addresses/passwords

<"mike martin" <mke.martn@gmail.com>>

Wed, 5 Apr 2006 18:43:20 +1000

A blunder by New South Wales police has led to a database of e-mail passwords being available on the Internet for as many as 800 people, including those of the anti-terrorism chief and hundreds of journalists.

The database appears to have been taken offline within the past month, but

is still accessible [e.g., mirrored elsewhere] through Google.

[Source:

Sydney Morning Herald, 5 Apr 2005; PGN-ed]

<http://www.smh.com.au/news/technology/police-secret-password-blunder/2006/04/05/1143916566038.html>

It is not clear why a police server would hold passwords of police and

journalists simply so they can receive police news releases.

And if it

does hold passwords, are they the same passwords as the people use to

access their own e-mail accounts. (Human nature being what it is, some

surely do.) Mike Martin, Sydney, coriaria.arborea@yahoo.com

✦ The risks of scaling incompetence to big numbers

<Poul-Henning Kamp <phk@phk.freebsd.dk>>

Sat, 08 Apr 2006 08:54:53 +0200

A swarm of D-Link products prod my NTP server despite the fact that they have never gotten an answer from it. I have spent nearly half a year trying to get D-Link to act responsibly and cover my costs but so far to no avail.

You can read my side of the story here:

<http://people.freebsd.org/~phk/dlink/>

A feature of modern fast-cycle product development and manufacturing is that a million defective products can be spread all over the market before anybody can get a chance to point out the defects.

In this case, the failure is relatively benign, and if D-Link covers the expenses it has cost me, no serious harm has come of it. But considering the lousy quality of software in these low-end devices, it is a safe bet that at least one or two of these products can be subverted as agents for a DoS attack.

In fact, only a few years ago, the NTP client component of NetGear devices did act as a DoS attack on University of Wisconsin, as some of you probably remember:

<http://www.cs.wisc.edu/~plonka/netgear-sntp/>

If risk to life and limb is involved, product recalls seems to happen automatically because the manufacturer fears litigation. The auto industry, Intels P5 divide instruction, hot and exploding lithium batteries, hot or flaming switchmode power supplies. The list goes on and on.

But unless a legal risk of significant magnitude is present, the vendor, like in this case D-Link, will not even reply to the complaint.

Here in Denmark buildings in which many people may be present, sports arenas, theaters and similar, must meet a higher standard in the building code than a regular house.

To my naïve mind, it would make a lot of sense if there were a legal requirement for a higher standard of product review and testing for high volume products in general, and legal liability should scale with at least $\log(\text{number_of_units_sold})$.

Poul-Henning Kamp phk@FreeBSD.ORG FreeBSD committer
BSD since 4.3-tahoe TCP/IP since RFC 956 UNIX since Zilog Zeus
3.20

Secure colocation in the North Sea

<Dan Jacobson <jidanni@jidanni.org>>

Thu, 30 Mar 2006 11:36:33 +0800

Hmmm, <http://www.havenco.com/>: "The Principality of Sealand is a former World War II anti-aircraft military fortress in the North Sea. Only authorized persons directly involved in the HavenCo project are permitted to land on the island. The Sealand Government is ideal for Web business, as there are no direct reporting or registration requirements."

"Tamper-resistant computing hardware, designed to protect customer transactions from all possible attackers, including HavenCo and its staff ... unmatched security, including 12" thick concrete walls, 24x7 armed security, and miles of empty sea between you and any threat."

Dan says: Probably hard to get spare parts to there during a storm though.

[PGN wonders whether there is remote access for maintenance purposes?]

✶ Classified military documents exposed through file sharing

<Diomidis Spinellis <dds@aueb.gr>>

Wed, 05 Apr 2006 19:23:59 +0300

The Greek newspaper *Eleftherotypia* in an article on April 5th 2006 [1], describes an interesting incident where classified Greek military documents became available on the Internet.

According to the article, an unnamed individual found on the Internet a number of military documents containing names of military units, details of mobilization procedures, and names and phone numbers of military officers. He notified the special forces chief of staff, and apparently thereafter all units that had active Internet connections were instructed to disconnect their machines from the network. Yet the individual could still access the files for hours, until he shut down his Internet connection.

Military sources explained that the incident occurred when an armed forces technician, while fixing a military unit's computer, copied the files to his laptop in order to burn them to a CD for backup purposes. He then forgot to remove them from his laptop's hard disk, and the files became exposed when he connected his laptop to the Internet through a private non-firewalled connection. The article's terminology doesn't clarify whether the files were shared on the Internet through Windows file shares or through a peer-to-peer file sharing program.

I would classify this story as a plain inept security management (what was a private laptop doing in an IT installation with classified documents?) were there not for the fact that the technician could conceivably be trying to do his job battling against other security measures. I can well imagine that the damaged computer was lacking a CD-ROM burner and a network connection as a (half-baked) security precaution.

[1] http://www.enet.gr/online/online_text/c=110,id=20584664 (in Greek)

Diomidis Spinellis - <http://www.spinellis.gr/>

⚡ Unexpected Internet Explorer behaviour when copy/pasting

<Pierre Pierre Blais <ppblais@yahoo.com>>

Thu, 6 Apr 2006 09:10:57 -0400 (EDT)

It's interesting that at the same time I was reading the recent postings about Excel's non-obvious behaviour, I ran into an unexpected Internet Explorer behaviour when copy/pasting.

I was visiting a Web page that has text only. It provides a list of on-line or webcast courses that one might be interested in taking. I needed to make a list of the courses I had taken.

Given that I had taken most of the courses, I highlighted the whole page and copy/pasted it into an Outlook e-mail I was composing, figuring all I needed to do was to delete the entries for the courses I had not taken.

I was quite surprised to see that more text was pasted than I thought I had copied. Some of the text was just repetition of what was already there. I blamed that on the copy process picking up both link destinations (HTML href) as well as the text itself.

However, I also noticed that the set of courses was much longer than what I

could see on the page. I quickly ran a "view source" on the page to see that the list is indeed much longer than what is visible, with some entries marked not to be displayed:

```
<tr height=0 style='display:none'>
```

So, IE actually copies all the text (presumably because it wants to be able to copy and paste the HTML) and since I pasted into a text-only document, it converted the copied HTML to text with the result that I am not getting what I was seeing on the Web page. A non-intuitive result.

Presumably, if I had pasted into a location that was not text-only, I would have ended up with the HTML...

I wonder how many sites use this technique to hide some critical information temporarily...

⚡ Re: Three days of San Francisco BART upgrade crashes ([RISKS-24.23](#))

<"Martyn Thomas" <martyn@thomas-associates.co.uk>>

Wed, 5 Apr 2006 15:59:52 +0100

PGN: "The new supposedly self-correcting software had passed all of its tests on the previous Sunday, but evidently the testing was incomplete. "

What would `_complete_` testing look like?

[Martyn, Many thanks for your good sense of humo(u)r. Knowing

that

testing is NEVER complete in the larger sense, this was clearly a cynical

comment on my part, leaving the reader to ponder whether

* the test requirements were incomplete (undoubtedly)

* the testing against those requirements was incomplete (most likely)

* the testing methodology was inherently incomplete (certainly)

* and so on.

PGN]

✉ Re: Rootkit: erosion of terms? (Slade, [RISKS-24.23](#))

<"Steven M. Bellovin" <smb@cs.columbia.edu>>

Wed, 5 Apr 2006 21:17:39 -0400

Rob Slade complains that the word "rootkit" is being misused to describe cloaking software. I believe that that usage is, in fact, historically correct, as counter-intuitive as that may be. Certainly, it had that meaning 5 years ago; see CERT Advisory CA-2001-05 (<http://www.cert.org/advisories/CA-2001-05.html>). Wikipedia's description of the origin of the word agrees, but that's a very large can of worms I don't feel like opening now... Asking Google 'define rootkit' yields both meanings, as does the Jargon File. But the last word may be in an article on a Symantec effort to standardize the definition (<http://www.computerpartner.nl/article.php?news=int&id=2353>):

But while efforts like the one Symantec is proposing may help professionals in the field, they will do nothing to alter popular usage,

said Alan Paller, director of research with the SANS Institute, a training organization for computer security professionals.

"I don't think you can stop the public and the marketing people from using words any way they choose," he said. "So even if there were a standard definition of a rootkit, it wouldn't change the use of the term."

Steven M. Bellovin, <http://www.cs.columbia.edu/~smb>

[And so it goes with many other terms:

- * "Virus" is used generically somewhat like "Kleenex" and "Xerox".

- * "Intrusion detection" typically applies to insiders and network denials of service that require no intrusion.

- * ...

Washington voting hijacked by computer mischief

<"Peter Gregory" <Peter.Gregory@concur.com>>

Wed, 12 Apr 2006 11:11:01 -0700

An online poll asking Washingtonians to pick their favorite design for the state's quarter coin was suspended, after the balloting was hijacked by computer programs whose automated scripts pushed the tally past 1 million votes over the weekend. [Source: Associated Press item, seen in *The Seattle Times*, 12 Apr 2006; PGN-ed]

http://seattletimes.nwsourc.com/html/localnews/2002923164_webquarter10.html

Peter H Gregory, Concur Technologies <http://www.concur.com> 1-425-702-8808

✶ Computer problems with U.Wisconsin voting system (Re: [RISKS-24.23](#))

<"Dana A. Freiburger" <dafreiburger@wisc.edu>>

Sat, 08 Apr 2006 13:41:40 -0500

An attempt to hold a campus election for the student council at the University of Wisconsin failed **again** due to "significant software errors", according to the University's Division of Information Technology (DoIT) group. According to their news release, "DoIT detected a disparity between the number of student votes cast and the number of votes confirmed in the online election database." No root cause was indicated in a DoIT news release and plans are being made now to run a paper-based election.

While the problem-struck online election system will "not be used again," there exists concern that the next attempt will suffer low turnout because of these computer snafus. Also, I noticed the local newspaper (the **Wisconsin State Journal**) did not offer an article on this event compared to the first time it occurred the previous week. Given that this newspaper is bored with this matter, voters can't be far behind.

The risks? Loss of respect for computer-based voting systems,

reduced
voter turnout due to these repeated problems, and continued
delays in
electing the next student council.

News from the University of Wisconsin's Division of Information
Technology: "DoIT Information on ASM Election Issues"

<<http://www.doit.wisc.edu/news/story.asp?filename=649>>

✶ Risks of email-to-fax services (Re: Ross, [RISKS-24.23](#))

<Jim Youll <jim@challengeandresponse.com>>

Wed, 5 Apr 2006 09:33:13 -0400

Dallman Ross ([RISKS-24.23](#)) wrote about the possibility of "Joe-
jobbing"
someone via the email-to-fax services that only authenticate the
e-mail
"from" address when sending (expensive) faxes.

The risks /appear to be/ mitigated such that real financial
damage to a
target is impractical, but the devil is in the details as I've
just
confirmed in examination of a large fax/voicemail service:

* This service (and JFax as well) once offered concerned
customers (me) the
option to place a text password inline at the top of the email
body, eg:

<password="SendMyFax007">. However, I noticed the password
string
sometimes leaked into the sent message, and its absence didn't
always
prevent a message going out. This "feature" doesn't seem to be
publicly
documented and was never user- configurable. I don't know if

it's still
available.

* The service under study this morning seems to update its authentications after a huge delay, if at all. I removed all references to an account's formerly authorized email address via the web page at 8:14am and replaced it with another. At 9:17am the service is still sending faxes received from the deleted e-mail address. So, even removing a compromised address doesn't stop the attack immediately. Inexplicably, it's referencing a "free trial account" now (the account was started as a free trial years ago). But it's charging the faxes against a real account, and logging them there.

* The services top-up a debit balance held at the service, then run it down before charging the credit card again. If you keep a low refill amount, this would throttle an attack, but the victim remains dependent on the company to "do the right thing" to reimburse.

* There is no way to stop faxes going out, and no way to remove stored credit card data or to stop the auto-charging of same. Attempts to erase credit card details yield a "you have entered an invalid credit card number" error. The service's contract requires that it be allowed to store credit cards and auto-charge both fixed monthly fees and per-use fees.

* The company cannot be easily reached by telephone, even in an emergency.

* The service allows account holders to disable notification of sent faxes. Presumably large account holders (those topping up with \$100 or \$250 per occurrence) thus wouldn't learn about an attack quickly. These accounts would presumably be the most in-demand.

* The service allows broadcast faxing on approved accounts, the fax equivalent of a spam relay.

I discussed these risks in 2002 with an architect of JFax, who is also a principal at another fax service. His (anonymized) comments below shed some light on their reasoning. He, and JFax before, considered this design necessary and reasonable given the limitations of both technology and customers. He's troublingly confident about the utility of "tracing an email back to where it came from" as a means of solving the problem.

"Yes, we've been through this one about a thousand times in the past. When we started (the service) back in 1996, we used to make the

sender place their customer ID and password in the subject line of the

email. We lost a lot of business because most folks could never figure out how to send a fax.

We do send a confirmation to your email address every time a fax is sent

on your behalf, so if someone is scamming your account, you should know

fairly quickly. Please inform us immediately and we'll credit your account

and trace the mail trail back to find out where the email came from.

This is a small risk that we have to face in order to do business in our

market. Fortunately it hasn't been too big a problem (stolen

credit cards

seems to be a much more real issue for us to deal with). In my dealings

with J2 (JFax)... I learned that they really hadn't had any issues with

this type of issue either. We'll keep our eyes open though."

✈ **Re: Man is charged \$4,334.33 for four burgers (Feit, [RISKS-24.23](#))**

<Martin Ward <martin@gkc.org.uk>>

Thu, 6 Apr 2006 10:23:44 +0100

> I suspect that's what happened in this case, and it's a very good reason to

> use a real credit card instead of a debit card.

When you use a credit card, the bank takes a cut of the transaction which mostly goes straight to their bottom line. When you use a debit card, their

cut is much smaller. So it is in the financial interests of the bank if

things happen to be arranged so that debit card transactions are risky, so

that people continue to give (valid) advice such as the above.

After all,

it's the customer's whether to use a credit card or a debit card, and it

doesn't cost the *customer* anything to use a credit card. The bank's gain

is the merchant's loss: but the merchant can't afford not to accept credit cards.

I'm not suggesting a great conspiracy on the bank's part: just a slight

disinclination to fix issues (such as the above) which are financially

beneficial to the bank. In other words: a definite conflict of interest!

martin@gkc.org.uk <http://www.cse.dmu.ac.uk/~mward/>

✶ Helios B737 Crash (RISK-24.23, Ferguson)

<Michael Loftis <mloftis@wgops.com>>

Tue, 04 Apr 2006 20:23:00 -0600

What Eric Ferguson has completely forgotten about is these huge looming things we call mountains out here in the mid western US. They're pretty solid, and descending into, or failing to ascend over, one of these is most always fatal.

I would completely refuse to be on an airplane with such an unsafe system in place. If it were to falsely believe there was a depressurization event while climbing out of say, Missoula, MT here, you'd certainly die. Lots of mountains to crash into.

A better solution would be some clearer warning signs as well as better training. It might not be a bad idea to have some form of mandatory hypoxia training though I have no idea how that could be done.

ANY system that impedes the pilots ability to control the airplane significantly for the sake of what the system designer thinks to be 'safety' will quite likely be far less safe than the original failure mode. Humans

are most usually far smarter than these systems.

✈️ **The 2005 Helios B737 Crash (Re: [RISKS-24.22](#) & 24.23)**

<David Alexander <dave_ale@online.rednet.co.uk>>

Wed, 05 Apr 2006 09:20:36 +0100

I can attest to the accuracy of the comments made about Time of Useful Consciousness. I have experienced hypoxia first-hand.

I trained as a pilot in the (UK) Royal Air Force. It may have changed in the last 25 years, but back then one of the first things we did in training was to sit in a chamber with an instructor to experience:

- 1) an explosive decompression from 12000 ft to (I think) 24000 ft
- 2) hypoxia

The idea is that you 'know your enemy' and can react properly if it happens for real.

I can tell you that hypoxia is very insidious and the effects are a lot like being very drunk, but it happens very quickly. You are sat in the chamber as a group after the explosive decompression, wearing an oxygen mask. 'One at a time they make you take your mask off and do exercises with pen and paper. You think you're doing fine and the effects haven't started yet, then the instructor puts the mask back on and you look at the complete garbage you have scrawled on the paper. The first third of the page is OK, then it

gets worse and worse - first in accuracy, then the handwriting looks like some thing a three year old would do, then there is a line off the edge of the page where you lost it completely (which is when they put your mask back on).

You experience it yourself and you get to see 9 other people go through it too. It's a very valuable lesson and one that ought to be taught to all pilots who fly planes that can exceed 12000 amsl.

[We have already received over a dozen messages on the Helios situation, from which this and the preceding one have been sampled. 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

Search RISKS using [swish-e](#)

Volume 24: Issue 25

Tuesday 18 April 2006

Contents

- [IE Changes Due: What You Can Expect](#)
[Gregg Keizer via Monty Solomon](#)
- [New Microsoft Patch Breaks Web Pages -- On Purpose!](#)
[Lauren Weinstein](#)
- [How to lose 10,000,000 pounds](#)
[Mike Williams via Mark Brader](#)
- [Norwegian bank has problems moving customers to new platform](#)
[Vetle Roeim](#)
- [Hong Kong: Former police complainants exposed on the Internet](#)
[John Kane](#)
- [Embedded Bug Detection](#)
[Al Mac](#)
- [Oxygen and autopilots](#)
[Andrew Koenig](#)
- [Another near-disaster due to vehicle automation](#)
[Pete Mellor](#)
- [Re: Another near-disaster due to vehicle automation](#)
[Don Norman](#)

- [Re: IT Corruption in the UK](#)
[Lem Bingley](#)
 - [DNS Amplification Attacks](#)
[Gadi Evron](#)
 - [Re: "routine" system failure](#)
[Ken Knowlton](#)
 - [Info on RISKS \(comp.risks\)](#)
-

IE Changes Due: What You Can Expect

<Monty Solomon <monty@roscom.com>>

Fri, 14 Apr 2006 15:37:54 -0400

Microsoft will release a security update for Internet Explorer that will also change how users interact with Web sites.

By Gregg Keizer, TechWeb.com, 11 Apr 2006

Microsoft Corp. will release Tuesday a security update for Internet Explorer that will also change how users interact with Web sites.

Some sites that rely on popular ActiveX controls, such as Apple's QuickTime, RealNetworks' RealPlayer, and Adobe's Flash and Acrobat, are likely to give users fits.

The change, which Microsoft has been warning Web site developers about since December 2005, was made to abide by a ruling in a patent infringement lawsuit Microsoft lost in 2003 to the University of California and its startup, Eolas Technologies Inc.

With the changes rolled out in a mandatory security fix, any IE

user who
downloads and installs Tuesday's security patches -- either
manually or via
an automated system such as Microsoft Update -- will likely need
to modify
how they use those sites which haven't been rewritten.

What should users expect? ...

[http://www.informationweek.com/story/showArticle.jhtml?
articleID=185300378](http://www.informationweek.com/story/showArticle.jhtml?articleID=185300378)

✦ New Microsoft Patch Breaks Web Pages -- On Purpose!

<Lauren Weinstein <lauren@vortex.com>>

Sat, 15 Apr 2006 09:42:31 -0700 (PDT)

OK, let's be fair about this, the underlying purpose of the
Microsoft patch
isn't to break Web pages, though this result was understood and
expected.

I haven't seen a detailed discussion of the implications of this
situation
in RISKS (some venues are calling the issue a "mini-Y2K" --
which is a bit
overdramatic), but it *is* important. As of a few days ago, vast
numbers of
Internet Explorer (IE) users are experiencing Web pages all over
the Net
which simply don't work as expected any more.

Simplified backstory first. A couple of years ago, Microsoft
lost a patent
fight over commonly used techniques to embed "active" content
into Web
pages. While "ActiveX" operations are usually cited in this
regard, in

reality all manner of embedded active player objects are apparently involved, including Flash, QuickTime, RealPlayer, Java, etc.

We can argue about whether or not such techniques should be patentable in the first place. A lot of us believe that such patents have gone way overboard and that the USPTO is far out of its depth.

In any case, MS decided that they didn't want to pay the associated license fees for the patented techniques (so far, the holders of the patent have seemingly not gone after open source browsers in non-commercial contexts -- such as Firefox -- which is why Firefox is not currently affected by this issue).

Several months ago, MS issued a patch to change IE behavior to what they believe is a non-infringing operation. This requires that users explicitly click embedded objects first (theoretically guided by a small hint message that appears if they happen to mouse over the objects, which will supposedly be visually boxed as a cue), before the objects will become active. In the case of active objects that already require a click to start, this means that **two** clicks will now be needed.

There are variations on this theme. For example, in some cases, playback of video may commence automatically, but the video control buttons reportedly won't be active unless the user clicks them first. Confusing? Yep.

There are ways to redesign Web pages to restore the original behaviors, more

or less. But these typically require the use of embedded javascript, which introduces its own complexity and security issues, especially on large sites.

If MS originally issued the patch that changed IE behavior months ago, why is this a big deal today? Because only now is Microsoft pushing out that patch as part of the standard automatic "Windows Update" mechanisms.

Previously, you would have had to manually download the patch yourself.

Millions of people are currently receiving the patch, and seeing the associated effects.

Now for an even more bizarre twist. Microsoft, realizing the sudden negative impact that this patch could have on many users, has just issued yet *another* patch (which as far as I know must be downloaded manually) that specifically *disables* the "offending" patch until the next planned IE update in a couple of months or so, restoring the original IE behavior until then on a temporary basis. Got that? You can't make this stuff up.

Perhaps the biggest problem with this situation is that many Web sites don't realize that they can be affected even if they don't use ActiveX. In fact, I wasn't aware of this until a few days ago, when I started having problems with a relatively simple embedded Flash video on one of my sites. You can see the effects and side-effects, plus the explanations I've now placed on the page, at:

<http://lauren.vortex.com/archive/000173.html>

Since the embedded video area is itself black, the new IE behavior of "boxing" the object as a cue to an additional click turned out to be essentially invisible. Surprise!

Note that the underlying display code is unchanged. I have not at this time added the javascript "container" code that would be necessary to "fully" workaroud this silly situation.

Are we all bozos on this bus, or what?

Lauren Weinstein +1 (818) 225-2800 <http://www.pfir.org> <http://www.ioic.net>

Blog: <http://lauren.vortex.com> DayThink: <http://daythink.vortex.com>

✶ How to lose 10,000,000 pounds

<msb@vex.net (Mark Brader)>

Mon, 3 Apr 2006 03:41:59 -0400 (EDT)

The following story was posted by Mike Williams, of the UK, a few days ago in rec.puzzles (without a usable email address where I could ask permission to forward it here). This copy was edited for typos.

I used to work on the S.W.I.F.T. payments system, and even that wasn't 100% perfect at eliminating duplicates and spotting omissions.

In the many years that I worked with the system, we had one situation where everybody followed the rules, and yet a payment for ten

million
pounds got lost.

It all started when an operator at Bank A mistyped 10,000,000 instead of

20,000,000 on the initial payment. The error was spotted pretty quickly -

banks have systems in place for double checking the total amount that gets paid in and out.

The operator could have sent a cancellation for 10,000,000 and a new

payment for 20,000,000 and all would have been well, but cancellations can

take days to process and someone would have to pay the overnight

interest. What actually happened was that they sent a second payment for

the remaining 10,000,000.

Now Bank A happened to use a system whereby the SWIFT Transaction Sequence

Number is the same as the initial paperwork that caused the payment to be

made, so the two payment messages were sent with the same TSN, the same

amount, date, payer and payee. In fact the two payment messages were

identical. (My bank didn't work like that, my programs always used a

unique TSN, but that's partly because I wanted to use our TSN as a unique

index on our outgoing files to make the coding simpler).

Unfortunately, at some point in its journey round the world, the initial

payment hit a comms glitch. These were the days when electronic data

communications were far less reliable than they are now. The relay station

didn't get a confirmation ("ACK") so it sent a copy of the message with a

"PDS" marker (Possibly duplicated by SWIFT network).

When the payments arrived at Bank B, they got passed to one of my programs

that checks the possible duplicates. Because the payments were 100%

identical, and one of them was flagged "PDS", that payment was dumped into

the "real duplicate" file.

Mike Williams, Gentleman of Leisure [Forwarded to RISKS by Mark Brader]

⚡ Norwegian bank has problems moving customers to new platform

<"Vetle Roeim" <vetler@gmail.com>>

Thu, 13 Apr 2006 13:26:39 +0200

After merging in 2003, the Norwegian banks DnB and Gjensidige NOR (now DnB NOR[1]), finally finished moving their customers onto a common platform earlier this year.

This did not go as smoothly as planned, though; in some cases company accounts and private accounts now require the same login, which in some cases have forced users to disclose their private accounts to others wanting to access company accounts[2].

In other cases, old access rights have been activated again. In one case a man had his account emptied by his ex-wife[3], and in another case a mother was granted access to her 37 year old sons account.

Both The Financial Supervisory Authority of Norway[4] and The

Data

Inspectorate[5] are a little cross with DnB NOR, and has asked them for more information about the problem. The bank, on the other hand, is trying to put a positive spin on the whole thing, claiming that all this is good for the customer and that it gives the customers better overview of their accounts[6]. Somehow I don't think their customers agree.

[1]: <URL:<http://www.dnbnor.com/>>

[2]: <URL:<http://www.vg.no/pub/vgart.hbs?artid=142282>>

(Norwegian)

[3]: <URL:<http://www.dn.no/forsiden/naringsliv/article756284.ece>> (Norwegian)

[4]: <URL:<http://www.kredittilsynet.no/>>

[5]: <URL:<http://www.datatilsynet.no/>>

[6]: <URL:<http://www.dn.no/privatokonomi/article753237.ece>> (Norwegian)

🚨 Hong Kong: Former police complainants exposed on the Internet

<"John_Kane@tricolour.queensu.ca" <John_Kane@tricolour.queensu.ca>>

13 Mar 2006 11:45:18 -0800

The identities of 20,000 former police complainants in Hong Kong have been made public on the Internet. The database, which contained highly confidential information, was discovered a few days ago on the website of a private company. The Independent Police Complaints Council has apologised for the security lapse and is currently conducting an investigation into the matter. Critics are now asking how the sensitive details were leaked in the first place. [Reported by Huey Fern Tay on Radio Australia's

Asia Pacific

web-page <http://www.abc.net.au/ra/asiapac/>]

✶ Embedded Bug Detection

<Al Mac <macwheel99@sige.com.net>>

Wed, 12 Apr 2006 01:33:21 -0500

[Much of this item will be familiar to old-time RISKS readers, but is

included to remind us that many old risks are still present. PGN]

Embedded bugs can kill people. Many bugs can be detected by thorough testing, or release the product without spending money on good testing, and wait until it kills people, then you know you got bugs. Guess which approach is most popular?

Software to analyse other software to detect Bugs is much in demand. How effective and economical is that state-of-art? As compared to doing proper testing, for example. Traditional software

(not embedded) has testing tools that can capture script of normal operations so as to test what happens after minor software changes.

It sounds like this kind of comprehensive automated testing is not in use where it is most needed.

At the Embedded Systems Conference in San Jose, California, attendees discussed how software practices can mean the difference between life and death. <http://www.embedded.com/esc/sv/>

* The Therac 25, designed to treat tumors with carefully targeted radiation,
killed three patients with radiation overdoses due to programming errors.

* Inspections of software after the crash of a U.S. Army Chinook helicopter
revealed 500 errors, including 50 critical ones, in just the first 17
percent of code tested. One wonders if the testing after the crash was
better than the testing before implementation, and if litigation will lead
to a better budget for testing before next disaster strikes.

* Electronic Smog is when instruments are inadequately shielded from
interference from other electronic instruments. Engineers have known of
this risk for decades, but new technology producers are perpetually
rediscovering this phenomena.

* A classic example of this is Japanese Bullet Train Doors opening when
passing Apartment Complexes due to lots of kids playing Electronic Toys.
This can kill passengers sucked out of the trains in the decompression.

* Pacemaker patients have had their devices inadvertently reprogrammed when
walking through metal detectors. In 2003, the pacemaker of a woman in
Japan was accidentally reprogrammed by her rice cooker.

* There have been a spate of problems with software in autos.

One report suggests that large software systems of more than a million lines
of code may have as many as 20,000 errors, 1,800 of them still unresolved

after a year. In my experience, such bugs are not evenly distributed, but are related to quality of programmers, programmer tools, testing, tech support (when alleged bugs are reported), project oversight, leading to clusters of systemic bugs some places, and almost total absence of bugs other places.

<http://www.informationweek.com/news/showArticle.jhtml?articleID=185300011>

<http://dso.com/news/showArticle.jhtml?articleID=185300246>

<http://biz.yahoo.com/prnews/060411/sftu082.html?.v=54>

✶ Oxygen and autopilots (Re: Ferguson, [RISKS-24.23](#))

<"Andrew Koenig" <ark@acm.org>>
Tue, 4 Apr 2006 22:58:09 -0400

> I would propose this Basic safety concept: before the system will allow
> itself to move into dangerous situations, the pilot must confirm that he
> is aware of the specific danger involved. [...]

As a (admittedly inactive) private pilot, I have to respond to this suggestion by saying "No way!!"

One reason is an even more basic safety concept: No autopilot or other device should ever be permitted to move the flight controls in ways that the crew cannot override. The reason is that it is impossible to predict all the circumstances in which a malfunctioning "safety device" might itself

cause a hazard that is impossible to prevent without overriding it.

More generally, automation tends to carry hazards in practice that do not exist in theory. For example, one light airplane manufacturer once came up with what looked on the surface like a wonderful safety innovation: Whenever the airplane is flying more slowly than a given limit, the wheels come down by themselves. No more gear-up landings, right?

Wrong. In practice, it turned out that the automatic gear extension mechanism failed more often than pilots forgot to lower manual gear explicitly, so there were *more* gear-up landings rather than fewer. Eventually, the FAA required the auto-extension system to be deactivated.

I can also imagine an altitude-based "safety system" forcing an airplane to fly into terrain if there is a sudden cabin depressurization that might have otherwise been survivable, or -- even worse -- if the sensor that measures cabin pressure malfunctions, indicating a depressurization when in fact none exists.

I see nothing intrinsically wrong with a cabin depressurization warning (and I imagine that pressurized airplanes already have them, though I've never flown one myself). I wouldn't even mind if an emergency depressurization instructed the autopilot to descend in case the crew were incapacitated--especially if the autopilot is coupled to a navigation system that knows enough to avoid terrain. But unless incapacitated, the pilot in

command should be in command.

✦ Another near-disaster due to vehicle automation

<Pete Mellor <pm@csr.city.ac.uk>>

Sat, 15 Apr 2006 00:09:24 +0100 (BST)

Don Norman contributed an item: "Motorist trapped in traffic circle for 14 hours" to [RISKS-24.22](#) on 1 Apr 2006. This reminded me of the following. I checked, and I was surprised to find that no one seemed to have reported it to RISKS, although it smells to me very much like an engine control system failure, and possibly a software failure.

It was widely reported in the UK press at the time. The following is one account by Nick Britten, which I found on-line, originally printed in the **Daily Telegraph**.

<http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/03/11/ntrapped11.xml&sSheet=/portal/2006/03/11/ixportaltop.html>

The comment by the driver regarding the power steering and the reaction of BMW, are particularly interesting.

- - - -

A motorist was trapped in his car driving at almost 130mph for 60 miles after the accelerator jammed. Kevin Nicolle, 25, was unable to stop the automatic BMW going at top speed after the malfunction on the A1. Kevin

Nicolle: 'I couldn't get the pedal off the floor' His terrifying journey, which was followed by four police cars and a helicopter, ended when he smashed the car into a roundabout, flipping it on its roof. ... Mr Nicolle was driving back from friends in Newcastle to his home in Southsea, Hants, last Sunday, when the accelerator on his automatic BMW 318 jammed at Catterick, near junction 53 of the A1. [PGN-ed]

Peter Mellor, Centre for Software Reliability, City University,
Northampton Square, London EC1V 0HB +44 (0)20 7040 8422

⚡ Re: Another near-disaster due to vehicle automation

<"Don Norman" <norman@nngroup.com>>

Fri, 14 Apr 2006 18:08:25 -0700

The BMW incident reported upon by Peter Mellor is eerily similar to the fake incident that I contributed to the April Fools' edition of [RISKS-24.22](#), 1

Apr 2006. My incident, which I carefully created to be as realistic as I could make it, fooled a few people. Moreover, I believe it could actually happen.

I was just in Cambridge (UK) and at a talk, I showed a slide of my fake news story. The audience responded by describing the BMW incident. There was some discussion that this particular auto has a "drive-by-wire" control: that is, the throttle pedal no longer has a mechanical link, but instead

signals the car's electronic control modules. In automobile language, this is called "Electronic throttle control": ETC. BMW calls it EDR, or possibly EMR. At least one aviation safety specialist at the Cambridge meeting said that his car has this, and he prefers it, because now throttle position controls speed, so that as long as the foot is held constant, the car maintains constant speed, even up and down hills. (And, if the newspaper story is correct, even if you take your foot off the pedal and attempt to apply the brakes.)

See RISKS for 1988: "Drive by wire" autos in development ([RISKS-6.48](#)). Yes, to answer a question asked in that RISKS submission, BMW did introduce electronic throttle control in their 7 series autos in 1988.

Caution: in the accident business, it is unwise to rely upon the initial newspaper reports. The official accident investigations, which can take a year or more to prepare, often have a very different slant on the incident. Perhaps Peter Mellor can follow up on this story when the official incident report is released.

Don Norman. www.jnd.org

[Later note from Don, Sun, 16 Apr 2006 18:41:40 -0700]

By the way. I did some more research on the topic. Seems that stuck throttles were a continual event with old, mechanical throttles. The electronic throttles have received numerous complaints, but all of the ones I could find were about "unintended acceleration". Doing a web search for

"electronic throttle accident" (without the quotes) is quite revealing.

I still don't know enough about this class of potential accidents to offer definitive comment. But from what I can tell, automobile incidents will replace aircraft ones for the RISKS community. The more things change, ...

Example:

The National Highway Transportation Safety Administration is investigating complaints that some Toyota Motor Corp. cars may suddenly accelerate or surge, causing one car to strike a pedestrian. The 2002 and 2003 Toyota Camry, Camry Solara and Lexus ES300 vehicles all come equipped with an electronic throttle control system, which the NHTSA said uses sensors to determine how much throttle is being applied.

The NHTSA said 30 crashes have been attributed to the problem, with four accidents resulting in five injuries. The crashes "varied from minor to significant and may have involved other vehicles and/or building structures." The preliminary investigation is the first step in the investigative process. The NHTSA will contact Toyota to ask for documents pertaining to the issue, and could upgrade the investigation to an engineering analysis. More than 1 million Toyotas are covered by this investigation, according to the agency.

Toyota officials could not immediately be reached for comment.

[Source: NHTSA Investigating Toyota Cars For Sudden Acceleration, Sharon Silke Carty, Accident Reconstruction]

<http://www.accidentreconstruction.com/news/mar04/030804d.asp>

✉ **Re: IT Corruption in the UK (Ravetz, [RISKS-24.23](#))**

<"Lem Bingley" <Lem_Bingley@vnu.co.uk>>

Fri, 7 Apr 2006 14:51:39 +0100

Jerry Ravetz's item (<http://catless.ncl.ac.uk/Risks/24.23.html#subj3>) on

Mapeley's involvement in Passport Agency biometric testing blurs the distinction between the current UK passport system, which uses a crude facial biometric process, and the upcoming biometric UK identity card system, which will undoubtedly be more complicated.

Mapeley may or may not become involved in the UK ID card project - the procurement phase has only just begun (see <http://www.computing.co.uk/computing/news/2153478/id-card-scheme-moves>).

At present the UK Home Office suggests that the eventual ID card will likely use a combination of facial biometrics and iris-recognition, which will obviously be much less prone to error than a facial biometric alone (the passport system compiles its biometric template from the photograph supplied on application, so is presumably fairly likely to spit out false positives). Obviously when I say there is less opportunity for error, I'm talking about the richness of information on which authentication decisions can be based, not the implementation of the system. Clearly you can

implement a system to create as many wrong decisions as you like.

I have wondered whether it might be possible to apply for two biometric ID cards, under different names, and escape detection.

According to one expert I've spoken to, iris-recognition applied to both eyes should be good enough to detect 99.99 percent of duplicate registration attempts - assuming there is a central register of templates where a new applicant can be compared with existing records. This is not yet certain for the UK system, but it is very likely. Again, the above level of confidence assumes the unlikely circumstance that there are no errors in implementation. (See http://lembingley.itweek.co.uk/2006/03/biometric_card_1.html for more).

Of course you may get away with applications for two ID cards if you turn up for each test wearing an eye patch - on alternate eyes.

Lem Bingley, Editor IT Week VNU BUSINESS PUBLICATIONS LIMITED,
32-34 Broadwick
Street, London, W1A 2HG +44 (0) 20 7316 9000 <http://www.itweek.co.uk>

DNS Amplification Attacks

<Gadi Evron <ge@linuxbox.org>>
Sat, 18 Mar 2006 03:50:44 +0200

In this paper we address in detail how the recent DNS DDoS attacks work:
how they abuse name servers, EDNS, the recursive feature and UDP

packet spoofing, as well as how the amplification effect works.

Our study is based on packet captures (we provide with samples) and logs from attacks on different networks reported to have a volume of 2.8Gbps.

One of these networks indicated some attacks have reached as high as 10Gbps and used as many as 140,000 exploited name servers.

In the conclusions we also discuss some remediation suggestions.

Given recent events, we have been encouraged to make this text available at this time.

<http://www.isotf.org/news/DNS-Amplification-Attacks.pdf>

Please note that this version of this paper is prior to submission for publication and that the final version may see significant revisions.

Randy Vaughn and Gadi Evron

✉ **Re: "routine" system failure (Magda, [RISKS-24.24](#))**

<Ken Knowlton <KCKnowlton@aol.com>>

Thu, 13 Apr 2006 20:59:55 EDT

I reacted, much as David Magda did, at the very odd notion of a "routine" system failure [in [RISKS-24.24](#)]. On further thought, an "ordinary" system failure (from buffer overrun, mishandled leap year, etc., etc.) can be meaningfully distinguished from a maliciously intended failure.

If the document had been translated into English (though it presumably wasn't in the cited case), a translator might not have understood the delicate difference between 'ordinary' and 'routine'. This thought makes me wonder whether troubles might not, many times, be compounded by insufficient vetting of translations of the technical reports of various misfortunes.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 26

Thursday 27 April 2006

Contents

- [MV-22 Tiltrotor Crash, March 2006](#)
[Peter B. Ladkin](#)
- [Verizon's Aggressive New Spam Filter Causing Problems](#)
[From Slashdot](#)
- [Congress readies new bill to expand DMCA, not shrink it](#)
[Declan McCullagh](#)
- [Triple DES Upgrades May Introduce New ATM Vulnerabilities](#)
[Redspin](#)
- [Another security/privacy breach at the University of Texas](#)
[PGN](#)
- [Super Bowl ticket scam](#)
[Connie Paige via Monty Solomon](#)
- [Opticon: A cheap way to get to work faster](#)
[Jeremy Epstein](#)
- [Radar for your PC](#)
[Erling Kristiansen](#)
- [RFID Zapper](#)
[Al Mac](#)
- [Personal Electronic Devices on Commercial Aircraft](#)
[Peter B. Ladkin](#)
- [PDF Hell for SA Bank](#)
[Colin Brayton](#)

- [HoneyPot Cars](#)
[Dawn Cohen](#)
 - [CfP: IEEE S&P special issue on malware](#)
[Ivan Arce](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈ MV-22 Tiltrotor Crash, March 2006

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>
Wed, 26 Apr 2006 11:11:57 +0200

On 27 Mar 2006, an MV-22 tiltrotor aircraft suffered a Class A mishap at Marine Corps Air Station New River, N.C. No one was injured but the aircraft was broken. The incident was reported in **Aviation Week**, 10 Apr 2006, p.29, as well as *Flight International*, 11-17 Apr 2006, p.9.

AvWeek says that during a post-maintenance check, the aircraft performed an unintended 3.1-second flight during which it climbed to about 7 ft altitude due to an engine/rotor overspeed. It descended rapidly, with the right landing gear taking most of the loads of the 9-fps impact. The right wing broke off at the root, as it is designed to do (the engine is at the end of the wing).

Flight International reports that the crew was switching between Full-Authority Digital Engine Controllers (FADECs) during pre-flight checks after an engine change. The selected controller failed, causing a power increase to one engine. The control system increased prop-rotor pitch to prevent an overspeed, which caused the aircraft to lift off rapidly. The system detected the failure and switched to the good FADEC after 2-3 seconds, causing loss of lift and the rapid descent.

According to **AvWeek**, Marine Corps Col. Bill Taylor said that the root cause is not yet known, but it is likely associated with the A-FADEC on the number two engine, as well as a "V-22 idiosyncrasy in how the aircraft handles an engine overspeed". It is hoped that revised FADEC SW will be

available and certified by October. AvWeek says that Goodrich is the FADEC supplier; Flight International reports that Rolls Royce is to modify the FADEC SW.

Peter B. Ladkin, Causalis Limited and University of Bielefeld
www.causalis.com www.rvs.uni-bielefeld.de

✈️ Verizon's Aggressive New Spam Filter Causing Problems (Slashdot)

<Monty Solomon <monty@roscom.com>>

Tue, 25 Apr 2006 08:08:57 -0400

[ScuttleMonkey on Slashdot:]

Aviancarrier writes "Verizon DSL has turned on a very aggressive spam filter

that is blocking lots of long-time legitimate e-mails. E-Mails get bounced

with an error: 'XX@verizon.net: host relay.verizon.net[206.46.232.11] said:

550 E-Mail from your E-Mail Service Provider is currently blocked by Verizon

Online's anti-spam system. The e-mail "sender" or E-Mail Service Provider may

visit <http://www.verizon.net/whitelist> and request removal of the block.'

That whitelist web page lets you request one address at a time to be whitelisted with no guarantee for their response time to process it. I have

tested multiple e-mail sources and only one got through. As a VZ customer, I

just spent 28 minutes on a call to tech support, eventually got a supervisor

who knows nothing about the new spam feature, and would only agree to e-mail

a manager who doesn't work weekends about it. I warned her that VZ has a public relations problem but she was too clueless to understand." Many users

have submitted this problem so it seems to be a pretty far reaching problem. There is also a discussion going on over at Google about this problem. ...

<http://it.slashdot.org/article.pl?sid=06/04/24/1538205>

✦ Congress readies new bill to expand DMCA, not shrink it

<Declan McCullagh <declan@well.com>>

Mon, 24 Apr 2006 14:34:28 -0700

I've placed the text of the draft bill here:

<http://www.politechbot.com/docs/house.dmca.copyright.bill.042406.pdf>

http://news.com.com/Congress+readies+broad+new+digital+copyright+bill/2100-1028_3-6064016.html

[Revised 24 Apr 2006]

For the last few years, a coalition of technology companies, academics and computer programmers has been trying to persuade Congress to scale back the Digital Millennium Copyright Act.

Now Congress is preparing to do precisely the opposite. A proposed copyright law seen by CNET News.com would expand the DMCA's restrictions on software that can bypass copy protections and grant federal police more wiretapping and enforcement powers.

The draft legislation, created by the Bush administration and backed by Rep. Lamar Smith, already enjoys the support of large copyright holders such as the Recording Industry Association of America. Smith, a Texas Republican, is the chairman of the U.S. House of Representatives subcommittee that oversees intellectual property law.

[...remainder snipped...] [by Declan!]

✦ Triple DES Upgrades May Introduce New ATM Vulnerabilities (Redspin)

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

Mon, 17 Apr 2006 12:23:30 PDT

[In the following 13 Apr 2006 press release, Redspin (an independent auditing firm based in Carpinteria, CA) suggests that the recent mandated upgrades of ATMs to support triple DES encryption of PINs has introduced new vulnerabilities into the ATM network environment -- because of other changes that were typically made concurrently with the triple DES upgrades. http://www.paymentsnews.com/2006/04/redspin_triple.html]

Redspin, Inc. has released a white paper detailing the problem. Essentially, unencrypted ATM transaction data is floating around bank networks, and bank managers are completely unaware of it. The only data from an ATM transaction that is encrypted is the PIN number.

"We were in the middle of an audit, looking at network traffic, when there it was, plain as day. We were surprised. The bank manager was surprised. Pretty much everyone we talk to is surprised. The card number, the expiration date, the account balances and withdrawal amounts, they all go across the networks in cleartext, which is exactly what it sounds like -- text that anyone can read," explained Abraham.

Ironically, the problem came about because of a mandated security improvement in ATMs. The original standard for ATM data encryption (DES) was becoming too easy to crack, so the standard was upgraded to Triple DES. Like any home improvement project, many ATM upgrades have snowballed to include a variety of other enhancements, including the use of transmission control protocol/Internet protocol (TCP/IP) -- moving ATMs off their own dedicated lines, and on to the banks' networks.

More and more banks now run their ATMs through their own computer network before the information goes on to a centralized processor. While having

the
ATMs on the bank's network instead of a bunch of individual, dedicated
lines
is much more economical and much easier to manage, it greatly increases
their security exposure.

The fact that ATM data isn't encrypted wasn't a problem when the
information
was going across dedicated lines, but now that it goes through the
bank's
Internet-connected system before going to a processor, it creates
unexpected
opportunities for crime and mischief. A hacker tapping into a bank's
network
would have complete access to every single ATM transaction going
through the
bank's ATMs.

"Our biggest concern is that not many bank managers know this," says
Abraham. "They assume that everything is encrypted. It's not a terrible
assumption, so it's no wonder that most bank managers we've talked to
are
unhappy to discover this after spending \$60,000 to upgrade an ATM.

"Fortunately," continues Abraham, "prevention isn't that complicated, as
long as bankers are aware that there is a potential problem. ATM
machines
need to be kept separate from the rest of the bank's computer network,
to
try to recreate that direct line to the processor. Also, Redspin is
developing a tool to help bankers determine their level of
vulnerability. This white paper is all about raising awareness."

✦ Another security/privacy breach at the University of Texas

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

Tue, 25 Apr 2006 15:34:42 PDT

Nearly 200,000 electronic records at the University of Texas at Austin's
business school have been illegally accessed, including SSNs and
possibly
bio info on faculty, students, staff, and alums. The previous breach

occurred in 2003, resulting in a former UT student receiving five years of probation and having to pay \$170,000 in restitution for accessing almost 40,000 SSNs. Last year, a former UT student received five years probation and was ordered to pay \$170,000 in restitution for hacking into the school's computer system in 2003 and accessing almost 40,000 Social Security numbers.

[Source: University of Texas Probes Computer Breach, Associated Press item, 23 Apr 2006; PGN-ed]

✶ Super Bowl ticket scam (Connie Paige)

<Monty Solomon <monty@roscom.com>>
Wed, 26 Apr 2006 00:15:24 -0400

Michael Deppe is facing six fraud charges. He reportedly offered tickets for the 2005 Super Bowl on the Internet for about \$7500 for a pair of seats, never delivered tickets to 68 people, and pocketed \$370,000. [Source: Connie Paige, *The Boston Globe*, 23 Apr 2006; PGN-ed]
http://www.boston.com/news/local/articles/2006/04/23/would_you_trust_this_man_to_sell_you_super_bowl_tickets_on_the_internet/

✶ Opticon: A cheap way to get to work faster

<Jeremy Epstein <jeremy.epstein@webmethods.com>>
Tue, 18 Apr 2006 06:38:45 -0700

It's been public information that there are devices ("Opticon" seems to be one brand name) that can cause traffic signals to turn green, intended for use by emergency vehicles. Not surprisingly, there are black-market devices

that send the appropriate signals (or perhaps they're the real thing, and not black-market).

What's interesting in the following article is that someone has been successfully using this technique for two years, and was fined \$50. Looking at it from a cost effectiveness perspective, seems that \$50 is a pretty good (albeit illegal) investment in getting where you're going faster for two years. IMHO, one has to be something of a sociopath to use such a device, because it's saying "my convenience is more important than yours" -- not very different from pushing to the front of a line in a grocery store or highway.

<http://www.cnn.com/2006/US/04/18/traffic.changer.ap/index.html>

Incidentally, in [RISKS-23.34](#), Russ Perry Jr mentions an interesting problem with emergency vehicles using Opticon devices approaching from two directions at once, but I couldn't locate any other references to this technology in the RISKS archives.

✈ Radar for your PC

<Erling Kristiansen <erling.kristiansen@xs4all.nl>>
Thu, 20 Apr 2006 21:05:13 +0200

From AVWeb, The Internet's Aviation Magazine & News Service
(http://www.avweb.com/newswire/12_16b/briefs/192056-1.html)

> With the AerFlight Virtual Radar
> <<http://www.aircraftspruce.com/catalog/avpages/aerflight.php>> system,
> just
> about any desktop PC can be turned into a virtual ATC-style radar
> screen. The AerFlight captures the Mode-S signals emitted by aircraft.
> Users can control parameters such as range, data displayed, waypoints
> and
> geographic outlines. Online databases provide extensive details for
> each
> aircraft. AerFlight VR software also can communicate with other users,

> providing real-time, live airspace traffic positioning around the
> world. The system is being marketed as a security asset and to anyone
with
> an interest in what's going on in the airspace above them, including
> flight departments, FBOs, flight schools and aviation enthusiasts.
Notes
> can be ascribed and activity histories stored. The system consists of
an
> antenna, receiver, and software package, and sells for about \$900.

[Mode-S is a so-called secondary surveillance radar data link that
returns
not only the identity of an aircraft, but also its 3-D position, and
maybe
some other flight data, in response to radar interrogation. I suppose a
similar device could be built to eavesdrop on ADS-B (Automatic Dependent
Surveillance - Broadcast), an emerging system in which aircraft
broadcast
their position, so ATC and aircraft in the vicinity can form a picture
of
the traffic - EK]

If I had any plans to interfere with flying aircraft in a violent
manner, I
would buy this device!

[According to a usually reliable RISKS reviewer, Mode S transponders
are
required to transmit pressure altitude (in 25-ft increments) but not
latitude-longitude, so a "3-D position" is not necessarily calculable
from
a Mode S transponder return. There is space in a Mode S return,
however,
to transmit additional data, such as lat-long coordinates from GPS,
if the
aircraft has these data and if they are desired for other protocols.

The transponder specs are publicly available from international
sources
(they must be: partly because they are administrative law in some
countries which require such equipment in commercial aircraft
operating
there). The basic returns are cleartext, public information, and
should
remain so (aviators like to know - are required to know - where
everyone
else is in the sky). Building a return-decoder as described is

technically

straightforward, and whether you put the SW in a proprietary avionics box

or sell it separately seems to me to be basically a business decision. SW

that deciphers transponder returns helps goodies and baddies alike.
PGN]

RFID Zapper

<Al Mac <macwheel99@sigecon.net>>

Thu, 20 Apr 2006 10:13:49 -0500

You might be interested in this development.
There is a window of opportunity for commercialization.
[https://events.ccc.de/congress/2005/wiki/RFID-Zapper\(EN\)](https://events.ccc.de/congress/2005/wiki/RFID-Zapper(EN))

As the title implies, some hobbyist has come up with what it takes for a paranoid person to obliterate any RFID tags that might be on consumer merchandise, or where not expected or wanted. You might also scroll to the bottom & read the CAUTION = ROFL.

I imagine that there will be a consumer market for this.

People who want one but do not have the personal what it takes to build stuff in their garage with assurance the contraption works right, and that they not injure themselves before getting it completed. Call this a niche industry that will attract a lot of imitators. To be profitable it needs mass production like on a circuit board assembly line.

- * Then the next market needed will be some way to assure purchasers that the RFID Zapper that THEY got really works.
- * Then the next society development will be that objects where RFID was inserted for purposes of identification, like in ID cards, Passports etc.
will malfunction because someone had used the RFID Zapper on them, rendering those people's ID unusable for the intended purposes.
- * Then stores, and other institutions, will have to institute rules that

people are not allowed to enter their premises carrying an RFID Zapper, so

as to prevent unauthorized usage on the store merchandise.

* Then the next result might be that RFID Zappers will get declared to be

illegal ... although I expect this will be a few years away ... the effort

to illegalize RFID Zappers may get a lot more attention from the general

public than the usual illegalization of technology tools.

There have been several problems with RFID deployment so far.

* There is the mass public panic over conspiracy theories, leading to a ton

of Urban Legends, of which there is a glimmer of validity at the fringes. There are in fact some risks of abuse, but they are relatively

small risks compared to the frenzy of claims out there.

* There's recent threads on the notion that el cheapo implementation can lead to security holes, where RFID is no exception to that risk, such as

susceptibility to malware.

* Spread of the RFID Zapper into society and its effects will become problem area # 3.

✶ Personal Electronic Devices on Commercial Aircraft

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>

Wed, 26 Apr 2006 10:56:31 +0200

There has been plenty of discussion of the risks of operating personal electronic devices (PEDs) such as mobile telephones, gameboys and computers

on board commercial transport aircraft. In the U.S., the use of mobile telephones on board flying aircraft is forbidden by the Federal Communications Commission, inter alia because such a phone would be within

receiving range of many cells simultaneously and the technology is neither

designed nor implemented to accommodate such cases. However, there is also

the possibility of interference with the aircraft avionics.

The subject was already brought to the attention of the RISKS community by Martin Howard in 1994 ([RISKS-16.23](#)), who quoted extensively from the monthly bulletin Callback for May 1994, published by NASA's Aviation Safety Reporting System (ASRS), an anonymised no-fault incident reporting system for aviation. Lars-Henrick Eriksson relayed an incident reported by the Swedish CAA in [RISKS-16.24](#). I have synopses of ASRS reports on the phenomenon from the late 1990's, as well as personal reports from commercial-pilot colleagues. I wrote a short article "Electromagnetic Interference with Aircraft Systems: why worry?", report RVS-J-97-03 in 1997, summarising much of this evidence and there was an article by Alfred Helfrick on the subject in Avionics News Magazine in September 1996. Both articles are available under the rubric "Do Passenger Electronics Interfere With Aircraft Systems?" in the compendium on Computer-Related Incidents with Commercial Aircraft (CRICA) on my group's WWW site www.rvs.uni-bielefeld.de. It is not a new issue.

More recently, the BBC reported on mobile phones and aircraft:
<http://www.bbc.co.uk/dna/h2g2/A6821318>

The article is helpful, but refers only vaguely to incident compilations, and doesn't provide any literature citations. It relates one incident in which a small commercial aircraft with seven passengers on board departed below the glideslope on an ILS approach into an airport in New Zealand in February 1993 and crashed. Despite being below the glideslope, the navigation instruments were indicating a descent, according to the article (that must mean that they were indicating that the aircraft was above the glideslope, even though it was in fact well below it). The pilot was calling on a mobile phone before the glide slope signal was acquired, and the call ceased when the aircraft crashed. There is no direct proof of interference but no other explanation for the incorrect nav indications has been offered.

Phones transmit whenever they are turned on, whether they are being used for a call or not. It is notoriously difficult to assess the strength or structure of enclosed electromagnetic fields, such as those formed by a transmitter in a more-or-less Faraday cage, and all the electrical wiring of the aircraft is contained within the cage. The U.K. CAA conducted some of the first studies on EM fields generated within aircraft by cell phones, reported in 2003 in CAA Paper 2003/3, available from http://www.caa.co.uk/docs/33/CAPAP2003_03.PDF A more recent report on PEDs and avionics from November 2005 is available at <http://www.caa.co.uk/docs/33/CAP756.PDF> This report references seven other documents from the CAA, JAA, RTCA, EUROCAE and a private body on EM interference from PEDs on board aircraft.

NASA wrote a technical memorandum TM-2004-213001 in 2004, "Evaluation of a Mobile Phone for Aircraft GPS Interference", available at <http://library-dspace.larc.nasa.gov/dspace/jsp/bitstream/2002/11768/1/NASA-2004-tm213001.pdf>

Recently, Bill Strauss, Jay Apt, M. Granger Morgan and Daniel D. Stancil have written an article on the subject for IEEE Spectrum, March 2006, entitled "Unsafe at any airspeed?", available at <http://www.spectrum.ieee.org/mar06/3069/1> as well as a Viewpoint for Aviation Week and Space Technology, April 10, 2006 (p.58). The authors are with the Naval Air Warfare Center (Strauss) and CMU. They conducted a study on passenger awareness of the issues, which showed that "passengers are not aware of the reasons for the limitations on inflight PED use. Many doubt that safety is an issue." They recommend expanding industry/government and inter-agency cooperation on the issue; augmenting the ASRS; characterising the in-flight radio-frequency environment more carefully; deploying simple real-time tools that will help pilots detect RF emissions; and clearly communicating the problems and dangers of PEDs to aircraft passengers. They conclude "our study has convinced us that use of personal electronics in

flight should continue to be limited and that no one should be allowed to operate intentionally radiating devices during critical phases of flight."

As many of us said a decade ago (see my op.cit.) In the meantime, the problem appears to have worsened thanks to the proliferation of PEDs, in particular intentional transmitters such as mobile phones, and the casual attitude most people seem to have towards their use. Thank goodness that colleagues are staying on the case.

Peter B. Ladkin, Causalis Limited and University of Bielefeld
www.causalis.com www.rvs.uni-bielefeld.de

PDF Hell for SA Bank

<"Colin Brayton" <cbrayton@gmail.com>>

Thu, 20 Apr 2006 10:43:21 -0400

Banks are warning clients who receive Internet "proof of payment" forms from First National Bank clients to physically check whether a deposit has been made, because a glitch in FNB's online banking software allows these forms to be altered by account holders.

And the bank doesn't know how long it will take to sort out the problem.

It has seemingly occurred because FNB opted for a printable document file (pdf) format for its downloadable "proof of payment" forms. These can be imported into Adobe Acrobat and the contents manipulated before being sent on to the recipient of the Internet transfer.

IOL<http://www.iol.co.za/index?set_id=3D1&click_id=3D13&art_id=vn20060417024758107C243105>

What do folks know about securing PDF documents? I know that encrypted and

password-protected PDFs are fairly easily cracked ... In a related story,

the U.S. Labor Dept. has an RFP out looking to convert XML to PDF.

Colin Brayton, Bklyn, NY <http://blogalization.nu/marketmachines>
<http://del.icio.us/marketmachine/news> cbrayton@blogalization.nu

🚀 Honeypot Cars

<Dawn Cohen <dawn.cohen@bms.com>>

Tue, 25 Apr 2006 13:45:03 -0400

Interesting use of honeypots in the real world: "bait cars" -- Reported on at <http://www.yahoo.com/s/297977> (which links to what I believe is a CNN report).

These are cars left out by police departments in car-theft prone areas, in hopes of catching car thieves. Cars include hidden video cameras to observe the thieves, GPS to track them, and a mechanism to lock the doors so that the thief cannot exit, until released by a cop (who will presumably arrest them). I'd have to worry about that last feature -- seems like a safety hazard, and may involve people besides the thief.

One major difference strikes me between this type of honeypot and the network honeypot: the attacker (thief) actually gets arrested for attacking the honeypot (stealing the car). The purpose of a network honeypot is to secure the real servers by identifying attackers/attacks. But presumably no one thinks of prosecuting an attacker who was not also caught attempting to attack a real server. Or do they?

<Ivan Arce <ivan.arce@CORESECURITY.COM>>

Tue, 18 Apr 2006 16:05:07 -0300

Subject: CFP: IEEE S&P special issue on malware

[Below is the Call for Papers for the IEEE S&P special issue on malware;

spyware, botnets, rootkits and other various forms of malware. The goal

is to have the final printer-ready versions of the selected papers by 4

Aug. Ivan]

Special issue of IEEE Security & Privacy magazine

Botnets, spyware, rootkits and assorted malware, September/October 2006

Deadline for submissions: May 31st, 2006

Guest editor: Ivan Arce (ivan.arce-AT-coresecurity.com)

The continuing evolution of security threats and countermeasures increasingly points at spyware, rootkits, botnets and a myriad of other software artifacts - loosely defined as "malware"- as the biggest challenge to achieve socially acceptable levels of security and privacy in today's IT environments.

The number of reported incidents and criminal activities attributed to malware is believed to be growing steadily every year clearly signaling a topic that merits more focused attention and in-depth analysis from the information security community.

Consequently, the technological, legal and policy-related aspects of malware are the topic of an upcoming special issue of IEEE Security & Privacy magazine.

We are looking for feature articles with in-depth coverage of spyware, botnets, rootkits and other related malware exploring the following ideas:

- * Malware detection, categorization and analysis
- * Reverse engineering and static/dynamic binary analysis of spyware, rootkits and other malware.
- * Malware containment and removal.

- * Advances in offensive and defensive malware technology
- * The global and large scale trends in malware
- * Malware economics and metrics
- * In-depth research and case-studies of specific rootkits, spyware or botnet systems.
- * Malware-specific computer forensics and incident response
- * Malware-specific legal, regulatory and policy considerations

The above list is not complete nor closed, authors are encouraged to submit articles that explore other aspects of malware.

Submissions are due May 31st, 2006 and will be subject to the peer-review

methodology for refereed papers of the IEEE Security & Privacy magazine. Submissions will be accepted using the IEEE Computer Society Manuscript Central site at <http://cs-ieee.manuscriptcentral.com>

Articles should be understandable to a broad audience of people interested

in computing in science and engineering. The writing should be down to earth, practical, and original. Authors should avoid theory, mathematics, jargon, and abstract concepts. They should not assume that the audience will

have specialized experience in a particular subfield. appearance.

Feature articles normally run from 4 to 12 magazine pages, including all text, the abstract, keywords, biographies, illustrations, sidebars, table

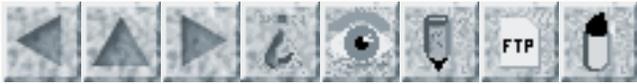
text, and reference entries. Articles should be between 4,500 to 7,000 words

(tables and figures count as 250 words each)

For more information see: <http://www.computer.org/mc/security/author.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

Search RISKS using [swish-e](#)

Volume 24: Issue 27

Monday 1 May 2006

Contents

- [Sounding the Alarm on Government-Mandated Data Retention](#)
[Lauren Weinstein](#)
- [Scarily Prophetic Ad](#)
[Daniel Graifer](#)
- [New Private Investigator laws for e-USA](#)
[Al Macintyre](#)
- [Japanese Newspaper subscriber information leaked to Internet](#)
[Glenn Story](#)
- [Drexel personal information on stolen laptop](#)
[Leonard Finegold](#)
- [Data storage firm apologizes for loss of railroad data tapes](#)
[Monty Solomon](#)
- [TSA: Computer glitch led to Atlanta airport scare](#)
[Patrick J. Kobly](#)
- [911 call show wrong address](#)
[John Curran](#)
- [Driven to distraction: cellphones](#)
[Monty Solomon](#)

- [Re: Man Gets \\$218 Trillion Phone Bill](#)
[Mathew](#)
 - [Re: PDF Hell for SA Bank](#)
[Seth Breidbart](#) [Jan Vorbrüggen](#)
 - [Trivia -- Truth Stranger than Fiction?](#)
[Chris Drewe](#)
 - [Re: RFID Zapper](#)
[Jan Vorbrüggen](#)
 - [Re: Triple DES Upgrades](#)
[Richard Outerbridge](#)
 - [Re: Honeypot Cars](#)
[Paul Robinson](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Sounding the Alarm on Government-Mandated Data Retention

<Lauren Weinstein <lauren@vortex.com>>

Sat, 29 Apr 2006 17:57:11 -0700 (PDT)

[A floor vote on this dangerous piece of legislation may happen as early as this Wednesday. This is a disaster in the making relating to flagrant disregard of privacy issues, data access without warrants, unconstrained dissemination and reuse, etc. The potential downsides are almost too numerous to list here! PGN]

Greetings. A few days ago, in this message:

<http://lists.elistx.com/archives/interesting-people/200604/msg00134.html>

I commented on Attorney General Gonzales' recent statement regarding data retention, and the alarming slippery slope that I feel this

represented.

Now, this article:

http://news.com.com/Congress+may+consider+mandatory+ISP+snooping/2100-1028_3-6066608.html?tag=st_lh

reports that a Democratic Congresswoman is proposing to fast-track a bill or amendment to *require* essentially permanent retention of users' Internet activity data (until at *least* one year after the user *closes their account*). For long-term users, this means effectively permanent retention.

Again, I must note the supreme ironies. It was only a few months ago that people were screaming bloody murder about DoJ demanding Search Engine records -- a demand that apparently only Google had the backbone to appropriately resist, noting the sensitivity of the data involved. This controversy triggered calls (including in some legislative quarters) for a law mandating the destruction of much related data after some reasonable, relatively short interval, with appropriate designated exceptions for R&D, business development, and the like.

Now, by waving the red flag of fighting child pornography, seemingly intelligent and usually well-meaning legislators appear ready to create the mother of all big-brother database laws, a treasure trove of personal data that will ultimately be available for every fishing expedition under the sun.

For those persons who trust the government not to abuse such

data, I hasten to note that these kinds of infrastructures, once in place, tend to be self-perpetuating, and will be available to *future* governments as well, including administrations who might not be as "benign" as the current one.

The article referenced above correctly notes the comparison with the McMartin Preschool child abuse witch-hunts of years ago. Hysteria over the abhorrent and real problem of child porn is being used to potentially decimate broad and critical privacy rights -- with the high probability of negative effects and consequences that are almost impossible to overstate.

If we do not maintain a balance between law enforcement goals (including but not limited to child abuse issues), and privacy rights, we will be flushing those rights we've had as law-abiding citizens down the toilet -- all in the name of seemingly laudable goals.

The Internet is rapidly becoming involved in most technology-based human communications. The sensitivity of Internet user activity data can be enormous. Broadly mandated data retention would move us drastically toward the realm of previously unimaginable "nightmare" scenarios (such as requiring the recording of all telephone calls, or the installation of government cameras in bedrooms -- both actions that could indeed be useful for law enforcement purposes).

Without wishing to sound melodramatic, I strongly assert that if we don't

take a stand now, we are likely to see the wonders of the Net repurposed into shackles that have the potential to undermine the very basis of our fundamental freedoms.

Lauren Weinstein +1 (818) 225-2800 <http://www.pfir.org/lauren>
Co-Founder, PFIR People For Internet Responsibility - <http://www.pfir.org>
DayThink: <http://daythink.vortex.com> lauren@pfir.org <http://lauren.vortex.com>

⚡ Scarily Prophetic Ad

<Daniel Graifer <graifer@earthlink.net>>
Wed, 26 Apr 2006 22:23:18 -0400

This Ad is REALLY SCARY....

<http://www.adcritic.com/interactive/view.php?id=5927>

[Illustrative of what is to come? Worth viewing if you have not yet seen it (it's been around for a while). PGN]

⚡ New Private Investigator laws for e-USA

<Al Macintyre <macwheel99@sigeom.net>>
Thu, 27 Apr 2006 12:24:56 -0500

Some computer professionals will need to get a Private Investigator license just to continue doing their computer work. I imagine this will also apply

to accountants and auditors, in fact anyone who analyses data that is on computer systems, on behalf of some other company, and perhaps people who work at software houses, computer retailers, whoever does repairs to computers, installations of new stuff. We will have to be asking suppliers of firewall, anti-virus, anti-spam, anti-spyware etc. if they have a PI license, otherwise it might be illegal to buy their products, and if there are no such suppliers, then it may be illegal to be protected against the cyber-criminals.

Companies will need to get an opinion from their lawyers, with respect to filing annual reports with the state and with government regulators. We are supposed to swear this data is correct under penalty of perjury, but it was derived by accounting and computer experts, not Private Investigators, but now it is illegal to get such data from people who are not Private Investigators? Does this also mean that Police Department personnel need to get a PI license before they may testify in court?

From Security in the news.

<https://thei3p.org/pipermail/security-news-html>

Forensic felonies, *The Register*, 26 Apr 2006

A new Georgia law aimed at private investigators now ``extends to computer forensics and computer incident response, meaning that forensics experts who testify in court without a PI license may be committing a felony''. The ``law requires all private investigators in the State of Georgia to be

licensed'', and is ``intended to prevent people from simply opening up shop and claiming to be PIs.'' However, the ``problem lies in both the definition and interpretation of what services can only be offered by a licensed PI, and how that extends into the electronic world.'' Forensic experts, by definition help individuals and business owners to find, the `cause and responsibility for ... losses and damage to ... property'', which is exactly how the law describes the duties of private investigators, meaning that under the new law forensic experts would be committing a felony in the course of their usual trade. Other states with similar laws include California, Arizona, Utah, Nevada, Texas, Delaware, and New York. An exception allowing attorneys, and those working directly under, as well as any in-house experts a business may have, provides protection for some.

http://www.theregister.co.uk/2006/04/26/law_change_for_pis

⚡ Japanese Newspaper subscriber information leaked to Internet

<Glenn Story <storyg@acm.org>>

Fri, 28 Apr 2006 10:08:57 PDT

The Mainichi Shimbun reported that information on about 66,000 subscribers (including names, addresses, phone numbers, dates of birth, and e-mail addresses) was leaked onto the Internet. This resulted from an employee

copying the data onto his own computer, which was thought to have been infected with a virus that exploited a vulnerability in the *Share* file-sharing application. [Source: *The Japan Times*, 28 Apr 2006; PGN-ed]
<http://search.japantimes.co.jp/cgi-bin/nn20060428a3.html>

⚡ Drexel personal information on stolen laptop

<Leonard Finegold <L@drexel.edu>>
Fri, 21 Apr 2006 15:31:34 -0400

We're informed that identity may be stolen up to 7 years after the present theft. And a colleague asked "if laptop be retrieved, will we be told?" --
as if they'd never heard of copying. LF

Date: Fri, 21 Apr 2006 14:32:44 -0400
From: Drexel Special Announcment <drexmail@drexel.edu>
Subject: Your Free CreditWatch Program has been Extended to Two Years

As you know, Drexel has been informed by Deloitte & Touche, an independent firm that has conducted regular audits of our financial statements since 2001 that a laptop computer stolen from an employee of Deloitte & Touche contained files with personal information on current and retired Drexel employees, including Social Security numbers and birth dates.

[Lengthy plug for Equifax Personal Solutions omitted... PGN]

Leonard X. Finegold, Physics, Drexel University, Phila. PA 19104
L@drexel.edu 1-215.895.2740

⚡ Data storage firm apologizes for loss of railroad data tapes

<Monty Solomon <monty@roscom.com>>

Sat, 29 Apr 2006 01:30:43 -0400

Iron Mountain Inc. has apologized for losing personal data, including Social Security numbers, for as many as 17,000 Long Island Rail Road employees and former employees. [Source: Chris Reidy, *The Boston Globe*, 28 Apr 2006; PGN-ed]

http://www.boston.com/business/globe/articles/2006/04/28/data_storage_firm_apologizes_for_loss_of_railroad_data_tapes/

⚡ TSA: Computer glitch led to Atlanta airport scare

<"Patrick J. Kobly" <patrick@kobly.com>>

Fri, 21 Apr 2006 09:47:03 -0600

A bomb scare that lead authorities to evacuate security checkpoints for two hours at Atlanta's Hartsfield-Jackson International Airport on 19 Apr 2006 was reported by the Transportation Security Administration director as the result of a "software malfunction". The detected device was part of a routine test, but apparently could not be located. The software was supposed to follow up with a "This is a test" message, but apparently failed

to do so. [Source: cnn.com, 20 Apr 2006; PGN-ed]

<http://www.cnn.com/2006/US/04/20/atlanta.airport/index.html>

You've probably seen this one a few times (certainly since it got picked up by Slashdot), but it seems strangely reminiscent of the SAC/NORAD incidents of June, 1980 and November, 1979 (particularly the 1980 incident). (See <http://www-ee.stanford.edu/~hellman/Breakthrough/book/pdfs/borning.pdf> and Neumann's "Computer-Related Risks" book.)

The risks seem obvious here - whether testing the alertness of operators (as the Atlanta incident) or the systems (as in the 1980 SAC incident), we have to think about the consequences of test data on operational systems...

911 call show wrong address

<"John Curran" <curranj@gmail.com>>

Fri, 21 Apr 2006 13:15:35 -0400

In the 21 Apr 2006 issue of *The Washington Post* there is a story about a man in suburban Maryland who was suffering chest pains and called 911. But before he could tell the operator where he was, he passed out. The emergency squad responded to the address shown for the phone number, but it was the main building for the company and the main was in an adjacent building. The emergency personnel searched the building but did not find anything. He was found dead in his office ten hours later by a

cleaning

crew person. So the identification information shown by some systems to the 911 centers is linked to the main switch and its location and not the physical location of the unit making the call.

<http://www.washingtonpost.com/wp-dyn/content/article/2006/04/20/AR2006042001923.html>

[This is not unusual, and clearly needs to be recognized as a risk. PGN]

⚡ Driven to distraction: cellphones

<Monty Solomon <monty@roscom.com>>

Fri, 21 Apr 2006 02:32:17 -0400

The National Highway Traffic Safety Administration and the Virginia Tech Transportation Institute tracked the behavior of drivers in 100 vehicles equipped with video and sensor devices.

The results: Inattentiveness caused by drivers using a cell phone, applying makeup, and being distracted from the road -- all caught on videotape -- cause nearly 80 percent of crashes and 65 percent of near-crashes, according to the study. Each distraction carried a different risk of causing crashes or near crashes: reaching for an object increased the risk by nine times; drowsiness by at least four times; and applying makeup by three times. The one-year study ... cited cell phone use and drowsiness as the major causes

of distraction. [Source: Kathy Uek, *Metrowest Daily News*, 21
Apr 2006;

PGN-ed]

[http://www.metrowestdailynews.com/localRegional/view.bg?
articleid=127986](http://www.metrowestdailynews.com/localRegional/view.bg?articleid=127986)

⚡ Re: Man Gets \$218 Trillion Phone Bill (Hatton, [RISKS-24.24](#))

<mathew <meta@pobox.com>>

Tue, 25 Apr 2006 11:02:50 -0500

> An interesting one this. Unless this got misprinted
> somewhere, they must
> have gone to 64-bit arithmetic to issue bills this big.

Far more likely is that their billing system is written in
COBOL, and uses
BCD arithmetic.

In fact, since errors of a fraction of a penny are significant
in telephony
billing, I sincerely hope that they use BCD, and don't run the
risk of
binary representation errors.

See also <URL:<http://www2.hursley.ibm.com/decimal/>>. This is how
financial
arithmetic should be done, and it's worth noting that the sample
benchmark
code simulates a telco billing system.

<http://www.pobox.com/~meta/>

⚡ Re: PDF Hell for SA Bank

<sethb@panix.com (Seth Breidbart)>

Thu, 27 Apr 2006 22:01:52 +0000 (UTC)

Any printable format can be counterfeited; even if the bank sent a protected PDF (and the protection worked), it could just be replaced with an entirely user-generated PDF.

There are two methods for a bank to supply something that resembles proof of a transaction:

1. Digitally sign a statement of transaction. This has the weakness that most people can't verify the signature.
2. Provide a token (preferably opaque) that when entered into the bank's web site, provides the bank's view of the transaction as shown in the bank's records.

✶ Re: PDF Hell for SA Bank ([Risks 24.26](#))

<=?ISO-8859-15?Q?Jan_Vorbr=FCggen?= <jvorbrueggen-not@mediasec.de>>

Fri, 28 Apr 2006 09:56:13 +0200

> What do folks know about securing PDF documents? I know that encrypted and
> password-protected PDFs are fairly easily cracked

Obviously, the only way of handling this is to digitally sign the PDF, and get the recipient to check the signature. However, if you put a legible note to do so on the PDF itself, the man-in-the-middle attacker

might remove
that while falsifying the date...somewhat of a catch-22.

In this context, it remains unclear whether the functionality built into the reader allows one to display only the signed portion of the document. If not, the attacker can add additional (unsigned) objects that overwrite some of the displayed data with whatever she needs for her purposes. Technically, the signature will be verified, but the recipient perceives something different from what is signed - the What-you-see-is-what-you-sign problem. There are, of course, ways to work around it (also in the context of PDFs), but they require investment and additional work at both ends of the chain.

Jan Vorbrüggen - MediaSec Technologies, Berliner Platz 6-8, D-45127 Essen
+49 201 437 52 52 jvorbrueggen@mediasec.de <http://www.mediasec.com>

⚡ Trivia -- Truth Stranger than Fiction? (Re: Norman, [RISKS-24.22](#))

<Chris Drewe <e767pmk@yahoo.co.uk>>

Wed, 19 Apr 2006 22:09:46 +0100

> ... "Rather interesting," said Lewis Carroll, spokesperson for the
> university, "several college buildings are quite off their correct
> location." Unfortunately, initial estimates for moving the buildings and
> roads to correct these discrepancies are too expensive, so, as Carroll

> puts it, "we will have to put up with these problems, but we
will annotate
> the map to show where these placement errors occur."

By coincidence (presumably!), the following item appeared in the
uk.railway
Usenet group recently. Background is that Colne and Skipton are
two small
towns in northern England, about 30 miles/50km north of
Manchester; they are
only about 12 miles/20km apart, but the railway line between
them was closed
some years ago, so although they retain their stations,
traveling between
them by train means taking an amazingly circuitous route -- you
could
probably do it quicker by bicycle.

Date: Wed, 12 Apr 2006 13:45:32 +0100
From: srbroadbet@btopenwold.com (Steve Broadbent)
Newsgroups: uk.railway
Subject: Re: Clitheroe-Hellifield

> Why did that line close in the first place? Was it something
to do with
> the (now abandoned) plan to extend the motorway?

When I was chairman of the SELRAP re-opening campaign group
(www.selrap.org.uk), the story we were told that held sway
locally was
that a BR [British Railways] network map was shown to Barbara
Castle, then
Minister of Transport, which showed, erroneously, the Skipton-
Colne line
missing and thus closed. Thus rather than admit the error to
the
Minister, the line was duly closed. It was not closed as a
result of
Beeching [plan for rationalisation of UK's railways in 1960s],
it did not
close till January 1970

Re: RFID Zapper ([RISKS-24.26](#))

<=?ISO-8859-15?Q?Jan_Vorbr=FCggen?= <jvorbrueggen-not@mediasec.de>>

Fri, 28 Apr 2006 10:06:47 +0200

> I imagine that there will be a consumer market for this.

Oh yes!

> * Then the next society development will be that objects where RFID was

> inserted for purposes of identification, like in ID cards, Passports etc.

> will malfunction because someone had used the RFID Zapper on them,

> rendering those people's ID unusable for the intended purposes.

Indeed so. And what are the issuers' and verifiers' fallback positions when this happens, be it inadvertently or on purpose, either by the holder or by a third party? At least ICAO has now woken up to the problem and is actively pursuing such fallback positions.

Imagine an A380 load of passengers waiting at US immigrations, and somebody uses an RFID zapper on the crowd, perhaps to make it easier for some of the passengers to enter the US illegally.

People are already not amused by the prices they have to pay for the "RFID-enhanced" ID documents (above 100 Euro / 125 USD), which is about 3-5 times the current pricing. Lifetime issues are also a continuing problem - nobody believes the chips will last the 10 years that are these documents'

lifetimes now. For frequent travelers, even the promised three years will be iffy.

> * Then stores, and other institutions, will have to institute rules that
> people are not allowed to enter their premises carrying an RFID Zapper, so
> as to prevent unauthorized usage on the store merchandise.

That won't help some other, commercially relevant scenarios. As a variation of the above, consider me running a pharmaceuticals warehouse for a whole saler in a commercial district, with my competitor on the adjoining property. Everytime a truck drives up to unload, I activate my device that will zap perhaps 30% of all RFIDs in the packages that are being unloaded. Now consider all ramifications of this, both business and regulatory. It's a nightmare.

Jan Vorbrüggen - MediaSec Technologies, Berliner Platz 6-8, D-45127 Essen
+49 201 437 52 52 jvorbrueggen@mediasec.de <http://www.mediasec.com>

✶ Re: Triple DES Upgrades (Redspin, [RISKS-24.26](#))

<Richard Outerbridge <outer@sympatico.ca>>
Fri, 28 Apr 2006 12:22:05 -0400

The gist of the item is correct, but the fact of the matter is that it's not 3DES itself that is causing the problems. The 20-year old magnetic stripe infrastructure is the root cause, and moving to chip-and-PIN is

the fix that everyone except the USA is in the midst of adopting. In stereotypical and steadfastly arrogant fashion, USA banks are refusing to move to chip-and-PIN, whilst at the same time refusing to accept any international liability for not doing so. Have our cake and eat it too, anyone? Softwood lumber, anyone?

It's widely expected that magstripe skimming fraud will migrate to and become a significant distinguishing feature of the US retail marketplace, if it isn't already. Of course, any costs - either way, to deploy chip or continue to swallow increasing magstripe fraud - will continue to be externalized by the Banks to their retail consumers: you and me.

However, the article is absolutely right on one account: there's no way to go chip-and-PIN without 3DES. If that requires a Windows update to effect, well, the US Supreme Court made that risk assessment for all of us some while ago.

✉ **Re: Honeypot Cars (Cohen, [RISKS-24.26](#))**

<Paul Robinson <paul@paul-robinson.org>>

Sat, 29 Apr 2006 12:47:56 -0400

They can be done in one of two ways. My home town of Arlington County, Virginia is using them.

First, the cars are put out on the street, legally parked, unlocked, with the keys in the ignition. Someone comes by, sees the car, gets in and drives off. Within one block the car is disabled and locked. The thief (and anyone with them) is busted red handed for stealing a car. Faced with them caught locked in the stolen car and video evidence of them getting into and driving off a car they have no legal right to be in, they always plead guilty.

My understanding is that when the immobilization feature is used it is done while the police are watching that particular vehicle and it's done within a very short period of time, say a block or two of the person driving off, the idea (I presume) is the police are going after the "low hanging fruit" of casual joyriders.

(Please don't think I'm considering this lightly. I've had a vehicle robbed from maybe ten years ago, and I had a (different) car stolen a couple of years ago. I had the unfortunate privilege of getting the vehicle back, the guy who stole it was caught (unfortunate because the car wasn't worth very much but was fully insured and it would have been better for me if the insurance company had paid me for the legitimately stolen car) and the fortunate privilege that the guy who stole it learned his lesson, he went out, found work and actually paid me back for all of the damages I had to repair on the car. The county sent me a check a few months ago.)

In the secondary case, cars are allowed to be stolen by

professionals, who
now move them to walk-away parking lots where they leave them
for a while in
case the vehicle has Lojack or other tracking systems to see if
the police
come after them. The police let the vehicle sit, and when the
other thief
comes to get it, they follow it to its destination and bust the
chop shop
operator (most vehicles are stolen for rendering because it's
worth more
disassembled as parts than the vehicle as a whole and the parts
are
untraceable). In this scenario, the police are not going to
immobilize the
vehicle or trap the driver because they want the driver to get
wherever it's
going so they can bust him (or her) and the theft ring.

> But presumably no one thinks of prosecuting an attacker who
was not also

> caught attempting to attack a real server. Or do they?

If you can catch them. Clifford Stoll tells in his book "The
Cuckoo's Egg"
about his efforts to discover why there was a 75c discrepancy in
billing
records on the computer system he was managing, and this lead
him on an
intercontinental chase for a cracker who was breaking into
various systems
and using some as gateways to others in an attempt to cover his
tracks.

A lot of cyber attacks are being run by botnets in which the
operator sends
one command out to a bunch of other "compromised zombie"
computers that are
then committing DDOS attacks, sending spam, storing warez, etc.
Because
they are using a non-logging intermediary, it's much harder to
catch them.
You have to find the zombies they are using, then trace the

incoming traffic
from those zombies (if you can). If the guy uses enough
intermediaries it
may be damn near impossible, at least for DDOS attacks.

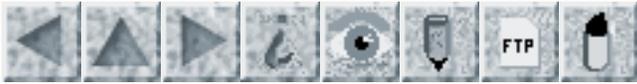
Basically, you need to "follow the money." Where there is spam
being sent,
someone is paying for the advertising, they need to be squeezed
to find out
whom they are using; if someone is doing a DDOS attack there
almost
certainly be an extortion demand, and the answer is to watch for
whomever is
coming to collect the money by flagging the transaction so they
can be
nabbed.

In both cases it's the same: catching someone who has to be
physically
present to commit the crime is trivial; they have to be there to
steal the
car and (in the other case) they have to be at some physical
location to
pull extortion payoff money from a transfer agent.

Compare that to catching someone who is using ten or twenty
thousand
compromised computers in ten thousand locations that may be in
places as
much as 1/2 way around the world from their actual location.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 28

Thursday 11 May 2006

Contents

- [The Problem of Test-Induced Failure & the Space Shuttle](#)
[Harry Crowther](#)
- [BA website discloses passenger passport numbers and DoB](#)
[Adam Laurie](#)
- [Open Letter to Google on Privacy](#)
[Lauren Weinstein](#)
- [Fraud in tampering with tamper-proof chip-and-PIN equipment](#)
[Nick Rothwell](#)
- [Re: Triple DES Upgrades May Introduce New ATM Vulnerability](#)
[Jim Daley](#) [Bill Cheswick](#)
- [NYPD deputy inspector caught rigging crime statistics](#)
[Ed Ravin](#)
- [Google Captcha](#)
[Mark Johnson](#)
- [Re: 911 call show wrong address](#)
[Ray Arsenault](#)
- [Bell inadvertently blocks 1-866 numbers](#)
[Rod Davison](#)

- [Re: Scarily Prophetic Ad](#)
[John Linwood Griffin](#)
 - [Re: New Private Investigator laws for e-USA](#)
[Stanley F. Quayle](#)
 - [In Wake of SAT Errors, Senator Seeks New Rules on College Testing](#)
[Karen Arenson via Monty Solomon](#)
 - [Spelling](#)
[Richard S. Russell](#)
 - [REVIEW: "Governance Guidebook", Fred Cohen](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ The Problem of Test-Induced Failure & the Space Shuttle

<"Harry Crowther" <hdcrowther@comcast.net>>

Sun, 7 May 2006 13:43:42 -0400

NASA managers decided on Thursday to skip a launch pad test of the shuttle

Discovery's redesigned fuel tank because of the risk the test itself could

damage the tank. The test would have entailed filling the shuttle's fuel

tank with cryogenic propellants and testing its systems. The fuel tank has

been the focus of NASA's shuttle safety upgrades since the 2003 Columbia

accident. [Source: Irene Klotz, NASA to skip shuttle tank test ahead of

July launch Reuters, 5 May 2006; PGN-ed]

There must be a better way. When there's doubt or trouble, skip the test

(!?!). There may indeed be some practical wisdom in evidence here, but it

doesn't bode well.

✦ BA website discloses passenger passport numbers and DoB

<Adam Laurie <adam.laurie@thebunker.net>>

Wed, 03 May 2006 14:43:53 +0100

In January of this year I reported to British Airways that it was possible to recover arbitrary passengers' confidential information, including Date Of Birth and passport details, by simply matching a frequent flier number to a surname when purchasing a ticket via their website. Since this information is printed on every boarding pass, any discarded passes can potentially provide an attacker with the information he needs to access the data via the website.

The problem exists because of the US Government's requirement for airlines to provide Advance Passenger Information for all passengers destined for their shores. It is left to the airlines themselves to administer the data collection systems, and, therefore, to make their own mistakes in the security systems that control access to that data. The more airlines that implement these systems, the more potential security holes will exist.

Full story here:

<http://www.guardian.co.uk/g2/story/0,,1766138,00.html>

Adam Laurie, The Bunker Secure Hosting Ltd., Ash Radar Station,
Sandwich, Kent

CT13 0PL UK <http://www.thebunker.net> +44 (0) 1304 814800

[Joel Baskin also noted

<http://www.guardian.co.uk/idcards/story/0,,1766266,00.html>

PGN]

✦ Open Letter to Google on Privacy

<Lauren Weinstein <lauren@vortex.com>>

Tue, 9 May 2006 15:50:28 -0700 (PDT)

An Open Letter to Google:
Concepts for a Google Privacy Initiative
Lauren Weinstein
May 9, 2006

<http://www.vortex.com/google-privacy-initiative>

Preface: The overall situation relating to U.S. and global privacy issues is deteriorating rapidly. Recent Congressional

moves toward legislating broad, government-mandated data retention laws (<http://lauren.vortex.com/archive/000175.html>)

are particularly alarming. The manners in which we collectively choose to address these sorts of issues are likely to have drastic impacts not only on our own lives, but

also broadly on the shape of society, both today and in the future.

Greetings. When I was recently invited to speak at Google's Santa Monica

center (Video at <http://lauren.vortex.com/archive/000168.html>), I was

impressed by the quality of the facilities, but even more so by the caliber

of the Google employees I met during my visit. Google's capabilities are

extraordinary. While I have been publicly critical of some Google policies, my concerns have been focused not on Google today, but rather mainly on how Google's immense data processing, storage, and related infrastructures might be abused in the future, particularly by outside entities in a position to force Google's hand despite Google's own best intentions.

As discussed in my talk, I consider Google to be an incredibly important and admirable resource with vast potential to do good. But by the same token, it is largely this very power that increases the risks of serious abuses of Google capabilities being forced upon the organization, and Google will likely be unable to mitigate many of these unless it takes major proactive steps on an immediate and ongoing basis, particularly including privacy-related efforts.

Increasingly, Internet users are becoming highly sensitized to both perceived and real risks to their privacy associated with their use of the Net. While the real risks we face in this arena are serious enough, people's confidence (or lack thereof) in products and services will in many cases be shaped primarily by perceptions, and often significantly less by the underlying realities. This highlights the critical fact that to be truly successful, efforts to reduce privacy risks must not only have genuine and ongoing positive privacy effects, but also need to be clearly perceived by users and the broader public to be in place and fully supported as primary goals of the organizations involved.

Web-based search engines are an obvious current focus of many privacy concerns, but as more traditional "desktop" applications migrate to tightly coupled topologies with user data stored on remote servers not under users' direct local control (e.g. for PC searches, document preparation, e-mail, etc.), these issues and related potential risks are rapidly spreading across the entire computer and Internet spectra.

Fears that users' private information may be increasingly subject to intrusive perusal by law enforcement or other authorities (often with minimal and/or questionable cause) are further damaging user confidence in such services, with a range of issues related to data retention being an important element at the heart of these concerns. To the extent that potentially sensitive data is stored for extended periods, particularly in non-anonymous forms, it is inevitable that outside demands for access to it -- on ever broader scales -- will be accelerating. While individual court cases will of course vary in their results, the court system cannot be relied upon to always render appropriate decisions regarding such matters, particularly in today's political and legislative environments.

I believe that Google, by virtue of its Internet industry leadership, technical and human resources, and corporate culture, is in a unique position. Google can demonstrate how world-class privacy protection policies and technologies can be developed and deployed in ways that enhance user confidence in current and future Google services -- by

proactively protecting users' private data without interfering with service operations, innovation, R&D, or the legitimate concerns of law enforcement. Google could be the acknowledged global leader in this area, becoming synonymous with the concept of integrating new and advanced privacy capabilities into world-class Internet services and products.

Obviously the confidence such efforts would engender in Google's users would be healthy for Google's bottom line, but more importantly it will provide genuine and continuing real benefits to the Google user community itself (i.e. the entire world). Where non-proprietary information is involved, further benefits to society could be achieved through making publicly available (via published papers, conferences, etc.) those aspects of resulting privacy-related R&D technologies that could be deployed by other entities to the benefit of the global community.

I recommend that Google establish a team explicitly dedicated to the development and deployment of privacy-related efforts as outlined above. Such a team would be tasked with establishing the framework of these projects in a consistent manner, and ensuring to the greatest extent practicable that all current and future Google products and services would be integrated (from the outset when possible) with these privacy technologies and policies. The team would need access to other individuals within both the development and operational aspects of Google, and ideally would report directly to high-level management.

To be effective, such a team would need to be significantly interdisciplinary in its makeup and scope, including a variety of skills.

Some of these would include a broad range of CS capabilities (including specialized mathematical disciplines related to encryption, among many others). Experience in dealing with the particular and complex interplay between technology and societal issues will also be an important component of such a team.

Google's growing scale and influence suggest that the sorts of privacy efforts suggested herein could be among the most important non-governmental privacy-related endeavors for many years to come, and could have vast positive impacts far into the future not only for Google and its users, but throughout the commercial, nonprofit, and government sectors.

This document represents a very brief conceptual outline, offered with only the best interests of both Google and the world at large in mind. Google and the broader Internet are at a critical crossroads in many respects, and I believe that Google has the opportunity to do enormous good by initiating the types of efforts that I've described.

I would welcome the opportunity to discuss these concepts with you in more detail and to work with Google toward their realization, as you may deem appropriate.

Thank you very much for your consideration.

Lauren Weinstein lauren@pfir.org <http://www.pfir.org/lauren> +1

(818)225-2800

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

⚡ Fraud in tampering with tamper-proof chip-and-PIN equipment

<Nick Rothwell <nick@cassiel.com>>

Tue, 2 May 2006 12:29:45 +0100

Something of a breaking story (currently being reported by BBC Radio 4's

"You and Yours" news magazine program, <http://www.bbc.co.uk/radio4/youandyours/>). Shell UK have withdrawn chip-and-PIN credit card

payment facilities from 160 of their garages, following incidents of

fraud. Chip-and-PIN has been publicised by the vendors as "safer, faster, more secure" than signature-based authentication (see the publicity at

<http://www.chipandpin.co.uk>), although the security of the PIN numbers is

the responsibility of the card holders. (This suggests that any fraud which

occurs puts the onus on the card holder to prove that the PIN number was not

divulged; with the old signature method, the onus is on the retailer to produce the sales slip.)

In this particular case, it appears that the card terminal devices designed

by Trintech, although tamper-resistant (i.e. will fail to operate if

tampered with), were tampered with to commit the fraud. Trintech are

claiming that their equipment is not at fault, and the issue is one of the

"environment" in which they were installed.

I am hoping that this story will be picked up by the science press, so that we can learn some of the details.

According to You and Yours, there have been previous incidents of chip-and-PIN fraud where unscrupulous retailers were able to add items to a customer's bill after the payment transaction.

nick rothwell -- composition, systems, performance -- <http://www.cassiel.com>

[Pete Mellor noted a BBC item on this:

<http://news.bbc.co.uk/go/pr/fr/-/1/hi/england/4980190.stm>

noting that this situation "rather dents the claim that the introduction

of chip-and-pin would dramatically reduce the level of 'plastic fraud'."

PGN]

Re: Triple DES Upgrades May Introduce New ATM Vulnerability (R-24.26)

<jdaley@cix.compulink.co.uk (Jim Daley)>

Sun, 7 May 2006 16:11 +0100 (BST)

If it really is only the pin that is being encrypted and it is accompanied with the account no - then isn't there an even greater risk of the bank's des keys being considerably more open to attack than in the past?

Effectively you have any number of ciphertext samples each corresponding to 4 digit pins, with repeat pins being easily identified by the account no,

also each ciphertext has a very limited range of equivalent plaintext (0-9999), and it wouldn't be too difficult to obtain a reasonable quantity of ciphertext with known plaintext by simply opening accounts in the compromised bank.

⚡ **Re: Triple DES Upgrades (Redspin, [RISKS-24.26](#))**

<ches@cheswick.com (ches)>
Mon, 1 May 2006 16:27:29 -0400 (EDT)

> In stereotypical and steadfastly arrogant fashion, USA banks are refusing
> to move to chip- and-PIN

I have heard briefings from highly-placed people at both MC and Visa discussing this. They are steadfast and firm: chips will not be implemented in the US credit cards. There is insufficient justification for the expense, given the cheap modems and phone system available to retail outlets.

⚡ **NYPD deputy inspector caught rigging crime statistics**

<Ed Ravin <eravin@panix.com>>
Wed, 10 May 2006 13:21:45 -0400

The *NY Post* reports that an NY City Police Department (NYPD) deputy

inspector was demoted down to captain after NYPD investigators concluded that he had rigged crime statistics when he was in charge of a Queens precinct in 2004. Full story at:

<http://www.nypost.com/news/regionalnews/63480.htm>

There have been previous reports of police commanders accused of falsifying the crime statistics (nicknamed "CompStat") in various ways, as they are under great pressure to show "good numbers", even if the criminals don't cooperate by committing less crimes. But this time there's a twist - the former inspector is also accused of "infiltrating the department's CompStat program to increase archived crime numbers for his precinct from before he arrived there" so that his ratings would look even better!

I'd love to hear the details about how the NYPD's database was altered - but the Department is rarely that forthcoming with its dirty laundry. They have stonewalled every outside investigation of this problem, especially the Mayor's Commission to Combat Police Corruption, whose chairman quietly resigned after the NYPD refused to cooperate with the Commission.

Most of the other reports involve rigging the statistics before the data is entered - felony crimes get "demoted" to lesser categories, and police discourage reports or "lose the paperwork" so that some crimes don't even get into the system in the first place. Even the head of the NYPD Patrolmen's Benevolent Association, the police officer's union, has complained about this.

The Village Voice published an excellent report that compared the police numbers with similar statistics from local hospitals, showing suspicious drops in assaults reported by the NYPD even though hospital admissions for assault were going up:

<http://www.villagevoice.com/news/0544,moses,69552,5.html>
<http://www.villagevoice.com/news/0544,moses,69552,5.html>

The RISK? The NYPD (and the many police departments worldwide who copy them) have become such slaves of their CompStat system that they spend their effort gaming it rather than doing their jobs and actually reducing crime.

[See also my post in [RISKS-13.69](#) describing how the NYPD plays similar computer games with a performance metric in their 911 dispatch system, online at <http://catless.ncl.ac.uk/Risks/13.69.html#subj7>]

[Another review of how the NYPD uses technology (including IBM Selectric typewriters!) is at:
http://www.baselinemag.com/print_article2/0,1217,a=30781,00.asp

(see the two articles "NYPD Rethinks its Dispatch System" and "The Disconnected Cop")]

Google Captcha

<"Mark Johnson" <mhjohnson@gmail.com>>
Wed, 10 May 2006 15:03:15 -0600

Apparently Google has been getting too many "automated" searches on their main site

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

or the personalized page at

<http://www.google.com/ig/>

and has added a "captcha" that you must answer prior to getting to the

search page. However, there seem to be some bugs including:

- repeated prompts for the captcha (about once per hour so far...)
- a frame with customized content is replaced by a Google error message that indicates your machine is possibly spyware or virus infected

I find it odd that Google would deploy something that prevents users from seeing all those advertisements that make money from the company (a side effect of doing searches). It would be interesting to find out the back story on this problem and why the "solution" is so broken for users of the search service.

[As a follow up, the captcha appears to have been removed after being up about four hours.]

⚡ Re: 911 call show wrong address

<"Ray Arsenault" <ray.arsenault@gmail.com>>

Fri, 5 May 2006 18:20:58 -0700

I think this is an issue not only with PBX's, but perhaps to a lesser extent CLEC's as well. I used to work for a business that had a

regular need for interaction with the City Police. In Vancouver (BC), if you need the city Police to attend anywhere, even if it's not a 911-type emergency, the only way to reach someone who can actually dispatch a car is to call 911.

Thus, I used to call 911 on a semi-regular basis, explain my issue-du-jour to the operator, and get the usual "We'll wander a car by when we have a minute, call us back if it escalates.."

But I also got more than my fair share of calls back saying either "We were at 401 West Georgia, and we can't find your business there..." or they'd call back a minute or so later and say "Uh, I thought you guys were over at (location). Our ANI says 401 West Georgia.."

We were using Allstream (formerly AT&T Canada), and I guess that their business offices in Vancouver were at 401 West Georgia, and so Telus (the ILEC) had that show up on ANI from thier trunks. I called Allstream repeatedly, and they just kept telling me "Well, we have your address as being (whatever), and so that's what should show up on ANI. There's nothing we can do about it."

⚡ Bell inadvertently blocks 1-866 numbers

<Rod Davison <rod@critsys.com>>

Tue, 9 May 2006 10:02:44 -0400

The 613 area code (Ottawa and eastern Ontario Canada) is moving from seven digit local calling to 10 digit local calling, a common transition. The first stage seemed to work okay with the caller id now showing the ten digits of local callers' numbers instead of the seven, but this morning, a new glitch appeared.

There is a local 866 exchange so that the phone number 866-1234 (just made up) is a local call. As of this morning, when I tried to dial 1-866-123-4567 I received the message "This is not a long distance call." as soon as I pressed the "4" in the sequence. Dialing "866-1234" got me the message "The mailbox of 866-1234 is full." I'm not really surprised.

In another several months, when full ten digit calling is required, this clearly will not occur. However, until then, one has to wonder about several issues:

(1) Why did Bell, or whoever else is involved, not test the possible effect of this change before it was made in the phone system. It is reasonable to assume that most 1-866 customers are businesses, which implies that this could have a significant impact on those businesses that rely on their toll free service to receive orders from customers and perform other business functions. The liability issue alone should have flagged this change as one that had to be tested thoroughly.

(2) When attempting to contact Bell about this issue, I received one of two responses. Either the Bell operator placed the call for me

without
listening to why I was calling, or they wanted me to schedule a
service
call. Finally after a number of attempts, someone at Bell
repair finally
"got it" and decided to relay my report to their supervisor.
When someone
reports unusual system behavior (and reports they observed it on
several
different phone lines) it should raise some sort of red flag.

Rod Davison, Critical Knowledge Systems Inc. (613) 834-7018
rod@critsys.com

 <John Linwood Griffin <griffin2@ece.cmu.edu>>
Tue, 2 May 2006 14:59:01 -0400 (EDT)

For those like me who would like to know more about where a link
goes before
clicking on it, this is the ACLU Pizza flash animation. Also,
for those
like me who had trouble accessing adcritic's web site, you may
go straight
to the source: <http://aclu.org/pizza/>

Re: New Private Investigator laws for e-USA

<"Stanley F. Quayle" <stan-at-stanq-dot-com>>
Thu, 04 May 2006 19:11:37 -0400

> Some computer professionals will need to get a Private
Investigator license

> just to continue doing their computer work.

The Ohio law requires this already:

The business of private investigation is [...] determine the cause of or responsibility for [...] damage to property, or to secure evidence for use in any legislative, administrative, or judicial investigation or proceeding.

> I imagine this will also apply to accountants and auditors

The law exempts, among other groups, lawyers and accountants.

> We will have to be asking suppliers of firewall, anti-virus, anti-spam,
> anti-spyware etc. if they have a PI license

Ohio law also exempts licensed professional engineers. Ask your supplier if they employ professional engineers -- after all, your software should follow sound engineering principles.

My signature line includes "P.E.", which stands for Professional Engineer.

Now I know why I got my license...

The Ohio private investigator FAQ:

http://www.homelandsecurity.ohio.gov/PISG_information/Classes_Licensure.htm

Stanley F. Quayle, P.E. N8SQ 8572 North Spring Ct.,
Pickerington, OH 43147

Quayle Consulting Inc. <http://www.stanq.com/charon-vax.html> 1-888-I-LUV-VAX

✶ In Wake of SAT Errors, Senator Seeks New Rules on College Testing

<Monty Solomon <monty@roscom.com>>

Wed, 3 May 2006 01:14:16 -0400

In Wake of SAT Errors, Senator Seeks New Rules on College Testing

[Source: Karen W. Arenson, **The New York Times**, 3 May 2006; PGN-ed]

NY State Senator Kenneth P. LaValle, chairman of the State Senate's higher education committee, said he would push for stricter government oversight of the college admissions testing industry, including a requirement that all questions and answers be disclosed after the exams without charge.

✶ Spelling

<"Richard S. Russell" <RichardSRussell@tds.net>>

Tue, 2 May 2006 15:15:37 -0500

Several of your recent correspondents seem to need this reminder:

"Lead" (pron. "leed") is present tense; "led" (pron. "ledd") is past tense; "lead" (pron. "ledd") is a heavy gray metal.

Just to confuse things:

"Read" (pron. "reed") is present tense; "read" (pron. "redd") is past tense; "red" (pron. "redd") is a color; "Redd" (pron. "redd") is a

guard for the Milwaukee Bucks.

Spell checkers will only flag the last item.

Richard S. Russell <http://richardsrussell.livejournal.com/> 608
+233-5640

[NOTE: RISKS cannot be responsible for such errors. Your moderator already fixes many typos, but cannot begin to attempt to overcome the growing general lack of attention to writing correctness. PGN]

⚡ REVIEW: "Governance Guidebook", Fred Cohen

<Rob Slade <rMslade@shaw.ca>>
Tue, 09 May 2006 11:53:57 -0800

BKCISOGG.RVW 20051119

"Governance Guidebook", Fred Cohen, 2005, 1-878109-34-0

%A Fred Cohen <http://all.net>

%D 2005

%G 1-878109-34-0

%I ASP Press

%O <http://www.amazon.com/exec/obidos/ASIN/1878109340/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/1878109340/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/1878109340/robsladesin03-20>

%O Audience a+ Tech 1 Writing 2 (see revfaq.htm for explanation)

%P 204 p.

%T "Governance Guidebook"

The very short section one of the Governance Guidebook explains that it is

intended for the CISO (Chief Information Security Officer) of a large concern. Which is to say that the reader should be experienced in security and the management thereof. At that point one wonders what such a work would entail: presumably such a person would already know pretty much anything you could put into a book. This introduction then goes on to detail the organization of the guidebook. Section two is an overview of the structure of a security plan or protection strategy. It also notes that the illustrations in this section of the text are very busy and cluttered, but that careful study will make the situation clearer.

All of this is true. This is definitely not your standard security textbook. It is extremely demanding of the reader, but will amply repay the effort put into using the volume. And I say "using," rather than merely "reading": this is a tome that requires application. Bed-time reading it is not.

This is not a primer to be read quickly in one sitting. The illustrations are dense, and so is the text, but dense with meaning and import. This is a work to be worked through, a page or even a paragraph at a time. And then, when you are finished, work through it again. If you are a CISO it won't teach you anything--but it will remind you of things, practices, and procedures that have possibly been forgotten in the press of other urgencies. This volume becomes, therefore, an aide memoire for the strategic planning of information protection.

This is not to say that there are no details provided. Section three, entitled "Drill Down," provides greater depth to a number of the areas (one example is an intriguing use of the human life span to address personnel and human resources issues). The content does not deal with specific technical areas of security, but does provide a very solid overview of security management--or, if you prefer, governance.

This is a handy and useful guide for those in the CISO position. It is destined to become well-thumbed, dirty, and dog-eared, over time. Those who are not yet into a CISO job will not recognize all of the value in its pages, yet. However, those who aspire to the calling would do well to get a start on learning from it.

copyright Robert M. Slade, 2005 BKCISOGG.RVW 20051119
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<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

Search RISKS using [swish-e](#)

Volume 24: Issue 29

Friday 26 May 2006

Contents

- [Amtrak halted by power failures](#)
[Patrick McGeehan via PGN](#)
- [Vast Data Cache About Veterans Has Been Stolen](#)
[Monty Solomon](#)
- [NASA's DART spacecraft smashes into satellite](#)
[Alicia Chang via PGN](#)
- [Predator UAV crash: switchology mistake](#)
[Mark M. Newton](#)
- [Expensive Australian navy avionics development failure](#)
[Rodney Polkinghorne](#)
- [Premiere of new opera delayed by computer malfunction](#)
[Mark Bartelt](#)
- [Planes, Trains, wait, did that sign say what I think it just said?](#)
[Trevor Paquette](#)
- [National Weather Center - Surface Winds from Bad Data](#)
[Ben Kamen](#)
- [Over-reliance on satellite navigation causes near-tragedy, again](#)
[Omri Schwarz](#)

- [Mandated Data Retention: Noble Goals With Evil Outcomes](#)
[Lauren Weinstein](#)
 - [Comcast outage leaves customers without TV, Internet & Phone service](#)
[Tim Duncan](#)
 - [Misunderstanding the risks of SSNs](#)
[Jeremy Epstein](#)
 - [Re: Another near-disaster due to vehicle automation](#)
[Mary Shafer](#)
 - [Re: Triple DES Upgrades May Introduce New ATM Vulnerability](#)
[Stephen Kent](#)
 - [Re: RFID zappers: zappers are not a new problem](#)
[Jerome Svigals](#)
 - [Re: Spelling](#)
[Dale Gombert](#)
 - [Re: Man Gets \\$218 Trillion Phone Bill](#)
[Barry Gold](#)
 - [Workshop on Trustworthy Elections: WOTE 2006](#)
[Peter Ryan](#)
 - [Electronic Voting Technology Workshop at USENIX Security](#)
[PGN](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Amtrak halted by power failures notsp

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

Fri, 26 May 2006 09:11:12 PDT

In the morning rushhour of 25 May 2006, circuit breakers cut out at 7:55am in Maryland, then in Queens, then in Philadelphia. By 8:03, Amtrak, New Jersey Transit, and (Baltimore-Washington) MARC trains were coasting to a standstill (without air conditioning, overhead lights, etc.). Four trains were stranded in the tubes under the Hudson River, another in a

tunnel in Baltimore. By evening, Amtrak officials were still unable to locate the triggering event, although it was noted that some of the electrical transmission equipment dates to the 1930s. Service was expected to return to normal on 26 May. The impact on commuters was of course severe.

[Source: Patrick McGeehan, *The New York Times*, national edition, 26 May 2006, C12; PGN-ed; Just one more reminder of the risks relating to an inadequately commitment to public transit, and the continued ability of single point failures to propagate? PGN]

⚡ Vast Data Cache About Veterans Has Been Stolen

<Monty Solomon <monty@roscom.com>>

Tue, 23 May 2006 00:51:29 -0400

Personal electronic information on up to 26.5 million military veterans, including their names, Social Security numbers, and birth dates, was stolen from the residence of a Department of Veterans Affairs employee who had taken the data home without authorization. [Comments about no evidence of data misuse (yet) and no health/financial records, but deeply embarrassing to VA. No mention of a statement that this incident was not reported for several weeks. The previous CardSystems Solutions breach in June 2005 was noted, affecting 40 million credit-card accounts. [Source: David Stout and Tom Zeller Jr., *The New York Times*, 23 May 2006 PGN-ed; yet

another ...]

<http://www.nytimes.com/2006/05/23/washington/23identity.html?ex=1306036800&en=eb1c02a63fedca31&ei=5090>

NASA's DART spacecraft smashes into satellite

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

Tue, 16 May 2006 15:13:15 PDT

NASA's 800-pound Demonstration for Autonomous Rendezvous Technology (DART) spacecraft was supposed to circle a defunct orbiting Pentagon satellite. A report released on 15 May 2006 indicates that DART moved to within 300 feet of the satellite 472 miles above Earth, and then lost control -- crashing into the satellite. The report says the collision was based on faulty navigational data from the main sensor that caused DART to "believe that it was backing away from its target" rather than approaching. Investigators concluded that DART had determined that it had spent too much fuel on the approach, because of the inaccurate data, and was in the process of shutting down when it collided. The investigation also concluded that the evaluation of fuel consumed was also in error (overestimated), and also faulted the mission's management style, lack of training and experience, avoidance of expert advice, and lack of internal checks and balances.

[Source: Alicia

Chang, AP item, Newsday, 15 May 2006; PGN-ed. Thanks to Lauren Weinstein

for spotting this one. PGN]

<http://www.newsday.com/news/nationworld/wire/sns-ap-spacecraft-mishap,0,4358085.story?coll=sns-ap-nationworld-headlines>

✈ Predator UAV crash: switchology mistake

<"Mark M. Newton" <newton06262@earthlink.net>>

Fri, 26 May 2006 04:56:10 GMT

The National Transportation Safety Board has released a preliminary report on the 25 Apr 2006 crash of a Predator UAV while on U.S. border patrol.

"The pilot reported that during the flight the console at PPO-1 'locked up', prompting him to switch control of the UAV to PPO-2. Checklist procedures state that prior to switching operational control between the two consoles, the pilot must match the control positions on the new console to those on the console, which had been controlling the UAV. The pilot stated in an interview that he failed to do this. The result was that the stop/feather control in PPO-2 was in the fuel cutoff position when the switch over from PPO-1 to PPO-2 occurred. As a result, the fuel was cut off to the UAV when control was transferred to PPO-2."

http://www.nts.gov/NTSB/brief.asp?ev_id=20060509X00531&key=1

✈ Expensive Australian navy avionics development failure

<Rodney Polkinghorne <rodneyp@physics.uq.edu.au>>

Mon, 15 May 2006 09:59:16 +1000

Dr. Brendan Nelson, Australia's minister for defence, has considered "getting out of" a billion dollar purchase of Super Seasprite helicopters, because "You could not have 100 per cent confidence in the software program that supports the pilot flying the helicopter to 100 per cent safety". He has upheld the ANZAC tradition of blaming the imperial overlords, US firm Kaman Aerospace and their subcontractors.

Full story in "The Australian" of 15th May 2006, online at <http://www.theaustralian.com.au/story/0,20867,19136512-601,00.html>.

Full disclosure: the author is a postgraduate student at an Australian university, and Dr Nelson was minister for education before he became minister for defence.

[Dr. Nelson is obviously also not a RISKS reader, or he would have ample evidence that "100% confidence" in a software program -- or even worse, in the system in which it resides -- is impossible. PGN]

✶ Premiere of new opera delayed by computer malfunction

<Mark Bartelt <mark@cacr.caltech.edu>>

Thu, 25 May 2006 16:24:49 -0700 (PDT)

The Los Angeles Opera was supposed to have been presenting the world premiere of *Grendel*, a new opera by Elliot Goldenthal this Saturday. Unfortunately, computer problems have forced a delay. A press release issued today says ...

"The technical rehearsals ceased on 23 May when computer malfunctions caused a large pivoting platform, central to scenery designer George Tsypin's large-scale set, to stop working, causing the platform's internal mechanisms to break. The platform, which uses 28 individually operating motors to move horizontally and vertically and pivot a full 360 degrees at a variety of speeds, must bear the weight of up to 15 performers at a time. Solving the malfunction of the computer system and correcting the failure has severely compromised the rehearsal time necessary for the success of the production, which demands extensive technical work."

<http://www.metoperafamily.org/operanews/news/pressrelease.aspx?id=1189>
http://www.losangelesopera.com/pdf/press_release/Grendel%20opening%20postponed.pdf

✈ Planes, Trains, wait, did that sign say what I think it just said?

<"Trevor Paquette" <Trevor.Paquette@TeraGo.ca>>
Fri, 5 May 2006 10:16:34 -0600

From the CBC link at: <http://www.cbc.ca/toronto/story/to-gotransit20060502.html>

Risks of an unprotected public electronic sign should be obvious...

GO Transit signs insult PM, CBC News, 2 May 2006

Technicians with GO Transit are working to make its electronic message boards hacker-proof after the scrolling signs were programmed to read "Stephen Harper Eats Babies" over and over again. Officials say someone used an inexpensive remote-control device to tamper with the narrow advertising signs installed in the system's trains along the Hamilton-Toronto route. The message was seen on Thursday and Friday, and appeared again on three separate signs on Monday.

Gerry Nicholls, one of the commuters who reported seeing the message, told the *Toronto Star* he thought he was "hallucinating" when he read it. None of the other commuters on the packed train seemed to react to it at, he said. As it happens, Nicholls is vice-president of the National Citizens Coalition, the conservative think-tank formerly headed by the prime minister. "I worked with Stephen Harper for five years and never once did he, in that time, eat a baby," he told the newspaper.

Text messages destined for the scrolling signs are transferred from a computer to hand-held, remote control device that retails for less than \$25. GO Transit employees then move from car to car with the device, transmitting the messages to the signs. GO Transit officials said they bought the signs six years ago and they were not password protected. It is the first time someone has hacked into the system, they said.

⚡ National Weather Center - Surface Winds from Bad Data

<Ben Kamen <bkamen@benjammin.net>>

Wed, 03 May 2006 12:53:32 -0500

Being a pilot and armchair meteorologist, I woke up Tuesday morning and did what I do every morning. I check the weather. I have various sinks bookmarked and one of my favorites is the ADDS system at <http://adds.aviationweather.gov/>

They have a Winds/Temps page at: <http://adds.aviationweather.gov/winds/> for which yesterday morning (Tuesday) the surface winds map showed this:

http://www.benjammin.net/www/images/ruc00hr_sfc_wind.gif

(saved on my website because I saved the .gif and mailed it to the site webadmins to let them know something was wrong even to my non-certified meteorologist eyes)

They e-mailed back (rather promptly I might add) to let me know that in fact the National Weather Service got bad data that morning and that the graphic was in fact wrong. NWS was working on fixing it.

Of course there was no mention on the website that something was awry with what I was seeing, but my own brain told me - "I don't think so!"

Thus, an interesting failure of mechanisms that gather data and transform it

into useful images for the rest of us. Mechanisms that apparently have no built-in method of error detection through a history of one input data set to the next.

I just thought I would share with the rest of you.

Ben Kamen - O.D.T, S.P. ben@benjammin.net <http://www.benjammin.net>

⚡ Over-reliance on satellite navigation causes near-tragedy, again

<"Omri Schwarz" <ocschwar@MIT.EDU>>

Tue, 16 May 2006 16:14:20 -0400

How many times have we seen this? How many more times will we see this?

The North East Ambulance Service is equipped with satellite navigation, which comes with the usual AI for giving driving directions. Said AI isn't fully informed on roads too narrow for the ambulance model. Said AI selects for short distances without factoring for traffic patterns and driving speed. Result: long delayed arrival at an accident scene and a delayed arrival at hospital afterward.

In this case the patient's mother offered to point out a better route, but was not allowed. A rapid response team that arrived before the ambulance did could have stayed with the ambulance and led a better route, but didn't.

[Source: British SATNAV service misdirects ambulance, *The Mirror*.

http://www.mirror.co.uk/news/tm_objectid=17083544&method=full&siteid=94762&headline=sham-bulance--name_page.html

Also noted by Joel Baskin, who included this pithy quote:

The service's patient forum said: ``SATNAV can be effective when used

with local knowledge. But it shouldn't be relied on by itself.''

PGN]

✈ Mandated Data Retention: Noble Goals With Evil Outcomes

<Lauren Weinstein <lauren@vortex.com>>

Thu, 04 May 2006 09:27:36 -0700

The irony of the situation relating to proposals for required data retention, as I noted in:

<http://lauren.vortex.com/archive/000175.html>

is that many incredibly bad and dangerous concepts -- like government-mandated data retention of this sort -- will virtually always be linked to laudable ideas (like fighting child abuse) that we all agree are important goals. A cynical view would be to assume that this is done purposely to push "evil" laws using "noble" hooks. This clearly does happen sometimes.

But I believe that in the majority of these cases we're dealing with legislators and others who genuinely believe in their causes, and either

don't have the will or background to recognize or understand the horrible collateral damage that their proposals would do.

Casting such persons as being purposefully evil is probably unproductive and unfair. Instead, we need to help them see the "big picture," rather than just the narrow focus of their good intentions.

For after all, the road to hell still does indeed remain paved with good intentions.

Lauren Weinstein: +1 (818) 225-2800 <http://www.pfir.org/lauren>
<http://lauren.vortex.com> DayThink: <http://daythink.vortex.com>

Comcast outage leaves customers without TV, Internet & Phone service

<tim.duncan@duncan.cx>

Sun, 21 May 2006 19:14:56 -0700

Thursday, May 18th, I turned on my TV at 8:00 PM to catch the final episode of "That '70s Show" only to find static. Checking another TV and finding only static as well I reasoned my Comcast cable TV was out-of-service. I tried calling comcast (800-COMCAST) to report the outage and only received a message that there was an outage in my area (I think they use caller id for this as I have received this message in the past when calling) and due to unusually high call volume all representatives were busy.

Since Comcast already knew of the outage I expected it to be

resolved in a little while and decided to pay some bills and check e-mail while I waited. Only then did I find out that my Comcast Internet was out as well. This is the first time an outage has affected both services I receive from Comcast.

A few calls to friends and family confirmed that service was out all over the Indianapolis area. Fortunately, as I was to find out later, my phone service is not through Comcast as it appears that all of Comcast's phone customers lost service as well.

It turns out a very localized power outage was to blame for the outage.

The Risk for customers? Putting too many eggs in one basket can cut you off from the outside world in a hurry.

The Risk for Comcast? Never assume your backup generator will be there when you need it. Test, test, test for power outages before they happen.

Some news reports of the outage:

<http://www.indystar.com/apps/pbcs.dll/article?AID=/20060519/NEWS01/605190512>

<http://www.theindychannel.com/news/9242765/detail.html>

✶ Misunderstanding the risks of SSNs

<Jeremy Epstein <jeremy.epstein@webmethods.com>>
Tue, 16 May 2006 07:06:19 -0700

Interesting article on recent congressional testimony regarding use of SSNs:

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9000482&source=NLT_AM&nid=1

I wasn't there, but based on the article there seems to be a serious misunderstanding that the SSN is just fine as an *identifier*; the problem is that it also gets used as an *authenticator*. Switching to a different number (as the article discusses) that is used for both purposes will have the same problem.

This quote sort of summed it up for me: "The Social Security number is the only unique identifier in our country that enables a credit grantor, or a credit bureau, or a bank, or an insurance company, or an investment firm to be sure that the consumer they are doing business with" is legitimate, according to Randy Lively Jr., CEO of the American Financial Services Association. In other words, they're using it as both an identifier and an authenticator.

Until Congress understands the problem, there's not much hope of solving it through legislation.

[Re: Another near-disaster due to vehicle automation \(Norman, R-24.25\)](#)

<"Reunite Gondwanaland (Mary Shafer)" <reunite.gondwana@gmail.com>>
Thu, 04 May 2006 07:22:47 -0700

> I still don't know enough about this class of potential accidents to offer
> definitive comment. But from what I can tell, automobile incidents will
> replace aircraft ones for the RISKS community. The more things change, ...

Once again, aviation was there first. I can't seem to find any details after all these years, but there was an incident with, I think, a Fokker airplane some years ago. I'm pretty sure I read about it in Flight International and it happened in Europe (or, at least, not in the US).

The WOW (Weight On Wheels) switch didn't make when the plane touched down, so the system wouldn't let the pilot throttle back. The pilot ended up going off onto the taxiway and then going back around onto the runway before bringing the plane to a halt, I think by pulling a circuit breaker. The impression the article gave was of an airplane zooming around on the ground while everyone else dove for cover.

I don't even think this was a fly-by-wire airplane, just one with safety interconnects. Another bit of evidence illustrating why adding back-up safety systems can make the entire system more dangerous. See Perrow on "Normal Accidents", for example. The article about the ValuJet accident, in Atlantic Monthly, was one of the best I've seen on this.

Mary Shafer Retired aerospace research engineer
reunite.gondwana@gmail.com or miliff@qnet.com

Re: Triple DES Upgrades May Introduce New ATM Vulnerability

<Stephen Kent <kent@bbn.com>>

Thu, 11 May 2006 17:17:05 -0400

(Daley, [RISKS-24.26](#))

Jim, I noticed your contribution to RISKS and just wanted to point out a possible misunderstanding re how PINs are encrypted in ATM nets.

DES (or 3DES) keys are used in these nets to compute a message authentication code (MAC) as an integrity and authentication check on a transaction between an ATM and a bank. The PIN is then XORed with the MAC to encrypt it. Thus one is not encrypting the PIN by passing it through the DES/3DES algorithm, as your text suggested. Rather, the algorithm is generating a pseudo-random bit string by virtue of being used to compute the MAC on a transaction. Each transaction contains a serial number, ATM ID, user account number, and other parameters that make the transaction likely to be unique, relative to the key that is shared on a pairwise basis between each ATM and a bank. Steve

Re: RFID zappers: zappers are not a new problem ([RISKS-24.27](#))

<"smartcard@sprynet.com" <smartcard@sprynet.com>>

Mon, 1 May 2006 18:14:57 -0400

The same challenge existed for magnetic striped cards in the

form of magnets

and magnetic field devices. they didn't succeed for a few reasons:

1) zappers hesitated to attach when it inconvenienced them selves. 2) the stripe or rf device is a pointer to a remote data base. after the zapping, the remote data base is still easily accessible. 3) there are always counterattacks to the zapping such as reduce range sensitivity and signal shielding.

jerome svigals (father of the magnetic striped card).

⚡ Re: Spelling

<"Dale Gombert" <GOMBEDWG@DFW.WA.GOV>>

Thu, 11 May 2006 15:15:05 -0700

A note of some significance here in the Pacific Northwest is that a "Redd" (pron. "redd") is a place salmon carve out of a stream bed to spawn. This (perhaps more universal) definition does not show up on dictionary.com, but a web search of "salmon redd" will supply many hits.

Dale Gombert <GombeDWG@dfw.wa.gov>, ITS4 WA Dept. Fish & Wildlife, Marine Resources, 16018 Mill Creek Blvd., Mill Creek, WA 98012-1296 1-425-379-2317

[Also noted by Al Stangenberger, UCB Center for Forestry. PGN]

✉ **Re: Man Gets \$218 Trillion Phone Bill (Mathew, [RISKS-24.27](#))**

<Barry Gold <barrydgold@comcast.net>>

Sun, 21 May 2006 06:34:09 -0700

> Far more likely is that their billing system is written in
COBOL, and uses
> BCD arithmetic.

I'm not impressed with the proposed representation. There is
no advantage
to representing things in decimal. You are representing
numbers, abstract
entities that exist independent of the base they are represented
in. In
any fixed representation, there will be limits -- a largest
(and smallest)
possible exponent, the maximum number of fractional bits/digits
that can be
represented. This can lead to either of two errors:

- * overflow: the number becomes too big for the representation
- * precision loss: the fraction is too long for the system to
represent, and
the least significant bits/digits are dropped, leading to
rounding errors.

One example would be calculating interest. Say you advertise a
rate of, say
2.75%, compounded daily. That means you need to divide .0275 by
365. The
result is an infinitely long repeating fraction, regardless
whether you
express it in decimal or in binary. Decimal only provides an
advantage if
you are dividing by 5 or 10, which produces a finite fraction in
decimal
notation but an infinite one in binary.

If you want to represent numbers without loss of either
significance
(overflow) or precision (rounding error), you can use any of

several
package, you can write in Franz Lisp, which allows arbitrary-
sized numbers
as a built-in type. Or you can use any of a number of arbitrary
precision
packages available on the web. Just do a search for the words
arbitrary
precision or rational arithmetic.

Using either of those techniques, you have no loss of either
precision or
significance(*) until the very end when you have to convert it
to money
units for billing and round to the nearest cent. But that is
inevitable
regardless of the representation you choose, an artifact of our
monetary
system which has no unit smaller than one cent.

* Until you run out of memory, if your calculation goes on long
enough
and the numerator and denominator get big enough.

✶ Workshop on Trustworthy Elections: WOTE 2006

<"Peter Ryan" <Peter.Ryan@newcastle.ac.uk>>

Fri, 12 May 2006 17:24:54 +0100

Workshop On Trustworthy Elections (WOTE 2006) Robinson College,
Cambridge, United Kingdom June 29 - June 30, 2006

<http://www.win.tue.nl/~berry/wote2006/>

Held in conjunction with

6th Workshop on Privacy Enhancing Technologies Robinson College,
Cambridge, United Kingdom June 28 - June 30, 2006

<http://petworkshop.org/2006/>

Announcement and Call for Contributions

The workshop is organized by IAVoSS, the International Association for Voting Systems Sciences, in association with the 6th Workshop on Privacy Enhancing Technologies. It follows in the tradition of the series of workshops devoted to cryptographic voting methods, such as WOTE '01, the DIMACS Workshop 2004, FEE 2005, and the NeSC Workshop on e-voting and e-democracy.

Scope and Objectives

Democracy and voting systems have received considerable attention of late, with the validity of many elections around the world being called into question. The US experience demonstrates that simply deploying technological "solutions" does not solve the problem and can easily exacerbate it. The aim of the workshop is to present and discuss promising technologies and schemes to achieve high assurance of accuracy and privacy in the casting and counting of votes.

The challenge is highly socio-technical in nature and requires an excellent understanding of the potentialities and dangers of technological approaches as well as an appreciation of the social, legal and political impact. The workshop thus aims to bring together researchers and practitioners from academia and industry as well policy makers, voting officials, whose work relates to electronic voting systems, to evaluate the state of the art, to share practical experiences, and to look for possible enhancements. The

overall aim then is to stimulate discourse between the various stakeholders and enhance the understanding of voting technologies and practices.

[See full announcement for suggested topics. PGN]

The workshop will consist of invited keynote presentations and contributed presentations. Panel discussions are also anticipated and submissions of suitable topics, with or without a moderator or example participants are welcome. The intention is to encourage plenty of discussion and so work in progress submissions are most welcome.

Accepted papers, abstracts and panel proposals will appear online. A separate category of presentations, Informal Communications, encourages preliminary ideas or status updates and requires only a short summary be submitted that may even relate to submissions to other conferences.

Our intention is to publish a special edition of selected papers in a major security journal. Acceptance of an extended abstract does not preclude publication elsewhere. Submissions from PC members are welcomed.

There will also be an opportunity to demo systems and prototypes the evening of Wednesday the 28th.

Contributions

To contribute a presentation, please submit an extended abstract summarizing a technical contribution or a position paper summarizing your research. Contributions will be selected by the expected interest in the

topic and the potential for stimulating exchange of ideas among the participants. A submission must be a PDF file of at most 8 pages, in letter-or A4-format, using at least 10pt fonts and no non-standard character sets. Submissions should be sent as an attachment by e-mail to peter.ryan@ncl.ac.uk.

All submissions must be received by midnight (UK time) 2 Jun 2006.

Notification of acceptance will be sent by 9 June, 2006.

General Chair: Peter Ryan (University of Newcastle, UK)
Program Chairs: David Chaum (Voteegrity, USA), Ron Rivest (MIT, USA)

P Y A Ryan
Professor of Computing Science
School of Computing Science
University of Newcastle
Newcastle upon Tyne NE1 7RU UK
Tel: +44 191 222 8972
Fax: +44 191 222 8788
peter.ryan@ncl.ac.uk
<http://www.cs.ncl.ac.uk/people/peter.ryan>

⚡ Electronic Voting Technology Workshop at USENIX Security

<"Peter G. Neumann" <neumann@csl.sri.com>>
Wed, 24 May 2006 16:37:11 PDT

For those of you going to USENIX and interested in the voting issues, an excellent workshop is being organized in conjunction with USENIX Security in Vancouver, and will take place on 1 Aug 2006. The program and other

information are already online.

<http://www.usenix.org/events/evt06/>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 30

Thursday 1 June 2006

Contents

- [EU blocks US access to flight data](#)
[Duane Thompson](#)
- [Computer outage hits Montana state government](#)
[Paul Goble](#)
- [Irish ATM pays double; ethical dilemma](#)
[Gerard McCarry](#)
- [\\$8 million for self-parking charge](#)
[Geoff Kuenning](#)
- [China fielding cyberattack units](#)
[Peter Gregory](#)
- [College Door Ajar for Online Criminals](#)
[Lynn Doan via PGN](#)
- [Computer c*ck-up finds e-r-e-c-t-i-o-n hard to handle](#)
[Nick Rothwell](#)
- [Why the Democratic Ethic of the World Wide Web May Be About to End](#)
[Adam Cohen via Monty Solomon](#)
- [Risks of Dishonest Hosting Providers](#)
[Roger Strong](#)

- [Nationwide's Website Refuses Customer Feedback](#)
[Chris Brady](#)
 - [Black Frog: next generation botnet. No generation spam fighting](#)
[Gadi Evron](#)
 - [Symantec Denies 'Highly Severe' Antivirus Flaw](#)
[Ed Sutherland via PGN](#)
 - [Re: NASA's DART spacecraft smashes into satellite](#)
[Robert P Schaefer](#)
 - [Re: National Weather Center ... Bad Data](#)
[Amos Shapir](#)
 - [Re: Comcast outage and backup](#)
[Craig Partridge](#)
 - [Re: Cellphones](#)
[Les Denham](#)
 - [Re: Google Captcha](#)
[Thomas Insel](#)
 - [Re: Over-reliance on satellite navigation](#)
[Matt Roberds](#)
 - [Re: Man Gets \\$218 Trillion Phone Bill](#)
[Marc Auslander](#) [Andrew Klossner](#) [Scott Peterson](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ EU blocks US access to flight data

<Duane Thompson <dst@rmhcn.org>>
Tue, 30 May 2006 06:08:51 -0700 (PDT)

Good for the EU! It seems that the EU will protect my privacy better than the U.S. will.

"The EU's highest court today blocked an agreement to give the US information about transatlantic air passengers. The European court of justice ruling said the US did not provide adequate protection for air

passengers' privacy. ..."

Guardian Unlimited, more at:

<http://www.guardian.co.uk/eu/story/0,,1786002,00.html>

Computer outage hits Montana state government

<"Paul Goble" <pg@pgcommunication.com>>

Wed, 31 May 2006 08:30:38 -0600

A hardware failure immobilized Montana state government from 1:30am on 22

May 2006 until 2:00am the next day. The hardware failure affected the "vast majority of services and computers" including things such as the state

Justice Department, drivers licences and wildlife permits.

Apparently key

services such as law enforcement were affected at first but were "rerouted."

Dawn Pizzini of the Information Technology Services Division is quoted as

saying, "We would have never assumed that that many components in that piece of equipment would fail."

<http://edition.cnn.com/2006/TECH/05/23/computer.outage.ap/>

http://www.helenair.com/articles/2006/05/24/montana/a08052406_01.txt

Paul Goble <pg@pgcommunication.com>

Irish ATM pays double; ethical dilemma

<"Gerard McCarry" <gmccarry@insightbb.com>>

Tue, 30 May 2006 21:57:25 -0400

The risk of taking advantage of a glitch

http://news.bbc.co.uk/2/hi/uk_news/northern_ireland/5019012.stm

✈ \$8 million for self-parking charge

<Geoff Kuenning <geoff@cs.hmc.edu>>

23 May 2006 14:29:53 -0700

A humor column in today's *LA Times* featured a photograph of a self-pay parking kiosk with a mis-set date of 16 May 1943, showing an amount due of \$8,082,022.84.

Sanity checking, you ask? Not bloody likely. An auxiliary display shows the fee in larger characters; it reads 8.1E+6. When you have an programmer so clueless as to calculate money values in floating point, there is little hope for subtleties like sanity checking.

As a side point, I'm fascinated that things like parking kiosks now use chips powerful enough to have floating-point support, at least as a library. A 4-bitter would be adequate for the task, though it's not clear to me that this particular programmer could have written the code needed to compute the fee on a 4-bit machine.

Geoff Kuenning geoff@cs.hmc.edu <http://www.cs.hmc.edu/~geoff/>

✈ China fielding cyberattack units

<Peter Gregory <petergregory@yahoo.com>>

Tue, 30 May 2006 15:07:24 -0700 (PDT)

From the nation that enjoys U.S. Most Favored Nation trade status, and a permanent member of the WTO...

China is stepping up its information warfare and computer network attack capabilities, according to a Department of Defense (DoD) report released last week. The Chinese People's Liberation Army (PLA) is developing information warfare reserve and militia units and has begun incorporating them into broader exercises and training. Also, China is developing the ability to launch preemptive attacks against enemy computer networks in a crisis, according to the document, ``Annual Report to Congress: Military Power of the People's Republic of China 2006.'' The Chinese approach centers on using civilian computer expertise and equipment to enhance PLA operations, the DoD report states.

Report: <http://www.defenselink.mil/pubs/china.html>

[Source: *Federal Computer Week*, 25 May 2006]

<http://www.fcw.com/article94650−05−25−06−Web>

College Door Ajar for Online Criminals

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

Tue, 30 May 2006 10:55:33 PDT

Hackers discover that universities are rich in personal data and easier prey than banks. Since January, at least 845,000 people have had sensitive information jeopardized in 29 security failures at colleges nationwide. ...

[Source: Lynn Doan, *Los Angeles Times*, 30 May 2006]

<http://www.latimes.com/technology/la-me-hacks30may30,0,1085392.story?coll=la-home-headlines>

Computer c*ck-up finds e-r-e-c-t-i-o-n hard to handle

<Nick Rothwell <nick@cassiel.com>>

Tue, 30 May 2006 17:40:52 +0100

Two e-mail messages objecting to a home extension failed to reach a council planning department because their computer system blocked the word "e-r-e-c-t-i-o-n". Commercial lawyer Ray Kennedy, from Middleton, Greater Manchester, claims he sent three e-mails to Rochdale council complaining about his neighbour's plans. But the first two messages failed to reach the planning department because the software on the town hall's computer system deemed them offensive. When his third e-mail, containing the same word, somehow squeezed through, it was too late. A planning officer told Mr Kennedy that his next-door neighbour's proposals had already

been given the
go ahead. [Source: *The Guardian* online, 30 May 2006; slightly
PGN-ed
to avoid filtering]
[http://society.guardian.co.uk/localgovt/story/0,,1786189,00.
html](http://society.guardian.co.uk/localgovt/story/0,,1786189,00.html)

Why the Democratic Ethic of the World Wide Web May Be About to End

<Monty Solomon <monty@roscom.com>>

Tue, 30 May 2006 00:21:10 -0400

(Adam Cohen)

Editorial Observer

Why the Democratic Ethic of the World Wide Web May Be About to End

The World Wide Web is the most democratic mass medium there has ever been. Freedom of the press, as the saying goes, belongs only to those who own one. Radio and television are controlled by those rich enough to buy a broadcast license. But anyone with an Internet-connected computer can reach out to a potential audience of billions.

This democratic Web did not just happen. Sir Tim Berners-Lee, the British computer scientist who invented the Web in 1989, envisioned a platform on which everyone in the world could communicate on an equal basis. But his vision is being threatened by telecommunications and cable companies, and other Internet service providers, that want to impose a new system of fees

that could create a hierarchy of Web sites. Major corporate sites would be able to pay the new fees, while little-guy sites could be shut out. ...

[Source: Adam Cohen, *The New York Times*, 28 May 2006]
<http://www.nytimes.com/2006/05/28/opinion/28sun3.html?ex=1306468800&en=cd83b09b58c721a6&ei=5090>

⚡ Risks of Dishonest Hosting Providers

<"Roger Strong (Computers)" <rogers@yetmans.mb.ca>>
Fri, 26 May 2006 15:52:38 -0500

Slashdot has a thread on Identifying and Avoiding Dishonest Hosting Providers:

<http://ask.slashdot.org/askslashdot/06/05/26/0034248.shtml>

One story that stood out:

"One place I looked at promised backup power. Then when I asked to see it, they explained that they only had the fittings and a contract for a backup generator that would be delivered in a couple of hours. Given that they are in San Francisco, that's a stupid plan, my-nurse-only-lets-me-use-a-spoon stupid; in an earthquake, their provider wouldn't have enough generators and probably wouldn't be able to deliver them anyhow."

Lesson learned: If your business depends on it being available, go tour the facilities. Verify that the generators, switching and back systems and redundant data pipes exist, and occasionally get tested.

⚡ Nationwide's Website Refuses Customer Feedback

<Chris Brady <chrisjbrady@yahoo.com>>

Wed, 31 May 2006 10:51:48 +0100 (BST)

Wishing to report a number of different phishing emails sent to Nationwide Building Society (UK) customers, including myself, I searched their website for a) an email address, &/or b) a feedback form. The urgency was to alert the technical team to get the false websites closed down. BUT there was NO contact email address on their website - not one. However I found a customer information request form but and a website feedback form. I duly completed both of these, including a cut & paste of the text of the offending emails, but with both when I clicked 'Submit query' I got the response 'Page Not Found.' I wonder how Nationwide stays in business when it can't even get a couple of feedback forms working. This is not the first company I've had similar problems with. It seems that few companies with a website presence actually want feedback from customers. CJB.

⚡ Black Frog: next generation botnet. No generation spam fighting

<Gadi Evron <ge@linuxbox.org>>

Thu, 25 May 2006 03:42:41 -0500 (CDT)

Black Frog - a new effort to continue the SO-CALLED Blue

Security fight

against spammers. A botnet, a crime, a stupid idea that I wish would have worked.

<http://news.google.com/news?q=black+frog>

Blue Frog by Blue Security was a good effort. Why? Because they wanted to "get spammers back".

They withstood tremendous Distributed Denial of Service (DDoS) attacks and abuse reports, getting kicked from ISP after ISP. They withstood the entire antispam and security community and industry saying they are bad.

The road to heaven is filled with good intentions. Their's was golden, but they got to hell, quite literally, non-the-less.

They did not hurt any spammer (okay, maybe one), as their attacks reaches servers spammers already moved from, domains spammers already dumped for the sake of thousands of other bulk-registered throw-away domains and so on.

Their attacks did reach hacked machines which hosted other sites. Their attacks reached ISP's with other users and their attacks hurt the Internet as well as these other legitimate targets.

Blue Security also got a lot of PR, good and bad, but they were not here first. Lycos Europe with their "make love not spam" effort was. ISP's globally null-routed that service, as it was indeed, much like Blue Security's, a DDoS tool by the use of a botnet. A botnet in this case being

numerous computers controlled from a centralized point to launch, say, an attack.

Lycos Europe soon realized their mistake and took their service off the air. Blue Security had 5 Millions USD of VC money to burn, so they stayed.

Even if they did reach spammers with their attacks (which they didn't), they would still hurt so many others with the attacks, and the Internet itself. When Blue Security came under attack they themselves said how DDoS attacks are bad, and their fallout hurts so much more than just their designated target.

That said, who is to determine said target?

When Blue Security went down, some of us made a bet as to when two bored guys sitting and planning their millions in some cafe would show up, with Blue Security's business plan minus the DDoS factor. Well - they just did.

Thing is, a P2P network is just as easy to DDoS. It has centralized points.

It is, indeed, a botnet.

I want to kick spammer behind too, but all I would accomplish by helping these guys is performing illegal attacks and hurting the Internet as well as innocent bystanders.

This business model will not last. It will get PR, but it will not be alone. 10 other efforts just such as this will follow. Now that

Black Frog

made their appearance - sooner rather than later.

How long is this journey of folly going to continue? Any service provider

which hosts them is as guilty of the illegal DDoS attacks as anyone who

signs up with them.

The way to kick spammer behinds is to, plain and simple, put them in

jail. I.e., change the economics. Make it more risky and less cost-effective

for them Bad Guys to spam.

I will keep updating about this latest useless harmful project on the blog

where this is written, <http://blogs.securiteam.com>.

Stop Black Frog Now.

Symantec Denies 'Highly Severe' Antivirus Flaw

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

Sat, 27 May 2006 10:52:50 PDT

Could Symantec's antivirus software guarding company, as well as government

computers include a backdoor allowing hackers access to corporate data? The

flaw could impact users of Symantec AntiVirus Corporate Edition 10.0 and

Symantec Client Security 3, according to eEye: the security vulnerability

can "compromise affected systems, allowing for the execution of malicious

code with system level access" and requires no user interaction. [Source:

Ed Sutherland, *Internet News*, 26 May 2006; PGN-ed]
<http://www.internetnews.com/security/article.php/3609501>

[A subsequent report on 31 May indicates that Symantec has fixed the problem. PGN]

⚡ **Re: NASA's DART spacecraft smashes into satellite ([RISKS-24.29](#))**

<"Schaefer, Robert P \ (US SSA)" <robert.p.schaefer@baesystems.com>>
Tue, 30 May 2006 11:25:48 -0400

An article titled "Multiple Errors Cause DART Rendezvous Mission Mishap",
Space News, 22 May 2006, states that the 70-page NASA report on this mishap will not be released because it contains sensitive material protected by ITAR. ITAR restrictions may also have been a contributing cause, i.e., people who should have talked to each other about technical issues/misunderstandings were prevented from talking to each other by law.

⚡ **Re: National Weather Center ... Bad Data (Kamen, [RISKS-24.29](#))**

<"Amos Shapir" <amos083@hotmail.com>>
Mon, 29 May 2006 18:01:20 +0300

Ever since the day weather observations were fed by phone or telex (5 bits per character, no parity bits or CRC) to weather centers where maps were drawn by hand, professional weather people have developed an

almost
instinctive ability to spot weird data, and ignore it when
analyzing weather
maps. Based on their experience, they could even make an
educated guess
about the possible correct values of bad data.

But letting some AI algorithm smooth out such data blips may be
Risky. What
if weather conditions did change abruptly? While stationed in a
desert
observation post in a previous life, I sometimes had to explain
to a
bewildered Air Force colonel that yes, the temperature here did
rise by 10 C
over the past half hour, and yes, the wind is 60 knots with zero
visibility
due to a sandstorm. Now try to explain that to a data-bot!

Nowadays there are many more situations in which professional
people are
taken "out of the loop", and data untouched by humans ends up
being
presented to lay people, including decision makers, who use it
without being
aware of its origin and quality. This is a known Risk, and
seems to be
unavoidable. In that case, it's better that these people be
presented with
raw data and be able to spot errors (like Ben Kamen did), than
automatically
processed data which might hide irregularities. When analyzing
weather
data, such irregularities are exactly what you don't want to
miss!

⚡ Re: Comcast outage and backup (Duncan, [RISKS-24.29](#))

<Craig Partridge <craig@aland.bbn.com>>

Tue, 30 May 2006 16:39:05 -0400

> The Risk for Comcast? Never assume your backup generator will
be there
> when you need it. Test, test, test for power outages before
they happen.

I just wanted to point out that testing the backup system
regularly does not
ensure it works. When we did the NRC study on the Internet's
performance on
9/11, I was surprised to learn that ISPs find that their backup
power
systems fail about 1 time in 10. (ref: "The Internet Under
Crisis
Conditions", p. 24, note 2). This is from ISPs that test
regularly (e.g.
once a month) and the number comes from their experiences with
the tests
(that is, in one test in ten, the backup system system doesn't
pick up
cleanly).

So the challenges are more subtle. How should an ISP invest in
and plan for
the recovery process for that 1 time in 10 outage? Designing
that process
right is hard. Example, one ISP I know had a policy of *NOT*
allowing
systems personnel into their facility immediately after the rare
case of
power loss and then being restored to key systems. Because
power loss was
such a rare event, the ISP used this experience as a chance to
audit
installation procedures that were supposed to ensure that
everything system
"just came up" when power was restored -- they'd often find a
system did not
just come up.

craig@aland.bbn.com or craig@bbn.com

Re: Cellphones ([RISKS-24.27](#))

<Les Denham <les@iiandt.com>>

Thu, 04 May 2006 00:42:18 GMT

> The results: Inattentiveness caused by drivers using a
> cell phone, applying makeup, and being distracted from the
> road -- all caught on videotape -- cause nearly 80 percent
> of crashes and 65 percent of near-crashes ...

That's an interesting conclusion.

Cellphones have gone from a rare luxury to ubiquitous in the last ten years.

Yet over the same time period, automobile accidents have declined steadily:

from 1994 to 2004 the fatality rate per 100 million miles has gone from 1.73

to 1.44, and the injury rate from 139 to 94. For cars (which are the most

common vehicles) the numbers for fatal crashes went from 2.07 to 1.57,

injury crashes from 191 to 123, and property-only crashes from 351 to 260

over the same period. (all statistics from

<http://www-nrd.nhtsa.dot.gov/pdf/nrd-30/NCSA/TSFAnn/TSF2004.pdf>)

I'd say the claim that cellphones are one of the major causes of traffic

accidents fails the basic test of common sense.

My guess -- based on personal observation -- is that the same idiots who

cause accidents by being distracted in other ways are the ones who cause

accidents involving cellphone use.

If, for example, a study finds 50% of accidents involve cellphones, that statistic is meaningless without a measurement of the proportion of drivers using cellphones. In Houston, where I live, informal observation suggests about 50% of drivers in rush hour traffic are using cellphones, and that doesn't count the ones using hands-free devices, or the ones with tinted windows.

⚡ **Re: Google Captcha (Johnson, [RISKS-24.28](#))**

<Thomas Insel <tinsel@tinsel.org>>
Thu, 11 May 2006 15:39:10 -0700 (PDT)

> It would be interesting to find out the back story on this problem and why
> the "solution" is so broken for users of the search service.

It's not generally deployed -- Google does this defensively when they see excessive traffic from a particular source address or network. Causes could include a virus such as MyDoom or an aggressive script.

I suspect that it's "broken" because they want to annoy you into fixing whatever's triggering the message.

⚡ **Re: Over-reliance on satellite navigation (Schwarz, [RISKS-24.29](#))**

<mroberds@att.net>
Sat, 27 May 2006 02:48:56 +0000

>The North East Ambulance Service is equipped with satellite navigation
>[which] isn't fully informed on roads too narrow for the ambulance model.

It is probably more cost-effective to modify the navigation software, but perhaps they should buy some narrower ambulances, especially if they are already aware of streets that are too narrow for their current vehicles.

<http://www.neambulance.nhs.uk/CommercialServices/Index/Index.htm>

shows a technician working on an ambulance that appears to be based on a Mercedes-Benz van that is sold as a Dodge or Freightliner "Sprinter" in the US. It appears that the cab is stock, but the ambulance box is wider than the stock van body.

http://www.cornermotors.com/images/sprinter_dimensions.jpg shows that the width of a US-model Sprinter, excluding the external mirrors, is either 76.2" (1935 mm) or 78.6" (1996 mm) depending on load capacity. By contrast, ambulances based on a stock Volkswagen Transporter, with a stock body width of 68.9" (1750 mm), have been successfully used in Europe.

Matt Roberds <mroberds@worldnet.att.net>

[For those of you who relish the risks of overly long vehicles, as

opposed to overly wide vehicles, this one is quite amusing.

<http://www.travelingtiger.com/tiensblog/2006/05/beached-suv-limo.html>

PGN]

⚡ Re: Man Gets \$218 Trillion Phone Bill (Gold, [RISKS-24.29](#))

<Marc Auslander <marcslists@optonline.net>>

Sat, 27 May 2006 10:33:16 -0400

"... I'm not impressed with the proposed representation. There is **no** advantage to representing things in decimal. ..."

In fact, there are serious practical programming advantages to decimal arithmetic in commercial programming. This is because the laws and customs related to rounding are stated in decimal terms. You can of course always get the right answer in binary, but it involves carefully scaling each number to the correct decimal precision so the rounding is correct. For example, many procedures need to be correctly rounded to the nearest mil, that is 1/1000 of a dollar. In binary, you need to represent amounts in mils to get the rounding right, then convert back to dollars and cents or dollars and mils for other purposes. In decimal, it all just works, of course.

[Some similar comments from Dik Winter. PGN]

⚡ Re: Man Gets \$218 Trillion Phone Bill (Gold, [RISKS-24.29](#))

<Andrew Klossner <andrew@cesa.opbu.xerox.com>>

Sun, 28 May 2006 21:26:38 -0700

> There is **no** advantage to representing things in decimal.

The advantage is that, when the system rounds or truncates values, it will do so in the way that customers expect. Rounding 0.142 dollars to 0.14 will surprise nobody.

> Say you advertise a rate of, say 2.75%, compounded daily. That means you
> need to divide .0275 by 365.

Never. Such accounts are compounded daily but credited monthly, when the calculation is $(\text{balance} * 0.257) / 12$, rounded to the nearest cent.

The rules of financial arithmetic have been codified for hundreds of years. They cannot be implemented using fixed binary notation. Arbitrary-precision arithmetic is completely impractical in data processing.

⚡ **Re: Man Gets \$218 Trillion Phone Bill (Gold, [RISKS-24.29](#))**

<Scott Peterson <scottp4@mindspring.com>>

Fri, 26 May 2006 14:08:21 -0700

At 11:30 AM 5/26/2006, Barry Gold <barrydgold@comcast.net> wrote

I think you're expressing opinions in without nearly enough information about the environment. For example, if this happened in a COBOL program running on an IBM mainframe your comments would be completely wrong because of the way data is typically stored and because of the way that these

computers most efficiently perform arithmetic.

> In *any* fixed representation, there will be limits -- a largest (and
> smallest) possible exponent, the maximum number of fractional bits/digits
> that can be represented.

And that's the job of a competent programmer. To make sure that the fields involved are large enough to hold any possible data.

> The result is an infinitely long repeating fraction, regardless whether
> you express it in decimal or in binary.

So? Pi is an infinite number but I can do calculations involving it with sufficient accuracy for my needs when I round it to 3 or 4 decimal places. I could care less what the rest is.

> Decimal only provides an advantage if you are dividing by 5 or 10, which
> produces a finite fraction in decimal notation but an infinite one in
> binary.

To me, this is so much gibberish. I think this simply shows unfamiliarity with how various computers work. Using IBM mainframes as an example, they do very efficient arithmetic in what's called packed decimal and that's a very common format for storing numbers. It's not as fast as binary, but when you add in the conversion factors it's generally faster. Floating point arithmetic is slower by orders of magnitude when you include the conversion overhead.

> If you want to represent numbers without loss of either

significance

> (overflow) or precision (rounding error), you can use any of
> several
> package, you can write in Franz Lisp, which allows arbitrary-
> sized numbers
> as a built-in type.

So your solution is to rewrite the program in an obscure
language on a
different platform. I think there would be easier, less
expensive
solutions.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 31

Monday 5 June 2006

Contents

- [Feds Continue Push For Mandated Internet Data Retention](#)
[Lauren Weinstein](#)
- [Re: Government-mandated data retention](#)
[Chris D.](#)
- [243,000 Hotels.com credit-card numbers stolen](#)
[Robert Heuman](#)
- [Data files erased at Aznar Government systems](#)
[Miguel A Gallardo](#)
- [Spam King Settles With Texas, Microsoft](#)
[Monty Solomon](#)
- [Risks of formulaic sanitization](#)
[Geoff Kuenning](#)
- [Re: NASA's DART spacecraft smashes into satellite](#)
[Peter B. Ladkin](#)
- [Re: \\$8 million for self-parking charge](#)
[Gabe Goldberg](#)
- [Re: Nationwide's Website Refuses Customer Feedback](#)
[Michael Hogsett](#)

- [REVIEW: "Software Configuration Management Using Vesta", Heydon et al.](#)
[Rob Slade](#)
 - [REVIEW: "Perfect Passwords", Mark Burnett](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Feds Continue Push For Mandated Internet Data Retention ([R-24.29](#))**

<Lauren Weinstein <pfir@pfir.org>>
Fri, 2 Jun 2006 08:28:06 -0700 (PDT)

<http://www.latimes.com/technology/la-fi-internet2jun02,0,622125.story?coll=la-home-headlines>

"The Justice Department said Thursday that it was not seeking to have the contents of e-mail archived, just information about the websites people visit and those with whom they correspond."

"Sounding the Alarm on Government-Mandated Data Retention"
<http://lauren.vortex.com/archive/000175.html>

This is a critical topic. The impracticality and cost issues associated with the new DOJ Internet data retention proposals are relatively obvious. It's difficult to even understand who would be required to comply with such demands. Only the big Web service companies? ISPs? (via packet tracking of their subscribers running their own servers?) Every small firm, organization, or even individual who operate their own e-mail and Web servers? Are the existing privacy policies of such entities instantly negated if they conflict with the DOJ wish list or data retention legislation?

It's also obvious how e-mail contact information could be abused. But there's something even more insidious in this situation. In the recent DOJ vs. Google case, Google and most unbiased observers correctly noted that "Web destinations" (URLs) frequently contain all manner of personal and private information. Names, addresses, social security numbers, dreams, hopes, interests, fears, medical queries -- all manner of details of our lives are embedded in the URLs we submit to search engines and other Web sites.

For all practical purposes, URLs in the Web context are very much like the content of phone calls in the conventional telecom context, judging by the level of detailed data that URLs provide and their ability to allow complete tracking of our every related Internet action in most cases.

If Internet users must live in fear that their actions on the Net are subject to retrospective analysis -- not only based on today's criteria but potentially on tomorrow's as well -- the effects on how we view and use the Net will be drastic, with vast unintended negative consequences that strike to the heart of our democracies.

This issue is ultimately more important than network neutrality, Internet governance, or most (if not all) of the other technically-related concerns that we bandy about here in IP or in most other forums, because it strikes to the very core of basic privacy concerns and personal freedoms.

Government-mandated Internet data retention could be the most potent single technological move in recent history toward enabling future tyranny against both individuals and groups.

We must not allow this issue to be "managed" through private meetings requested by government officials, or as a mere footnote in the public discourse or hastily passed legislation -- to be treated as a fait accompli by this or future administrations.

Lauren Weinstein +1 (818) 225-2800 <http://www.pfir.org/lauren>
PRIVACY Forum - <http://www.vortex.com> DayThink: <http://daythink.vortex.com>

✶ Re: Government-mandated data retention ([RISKS 24.29](#))

<"Chris D." <e767pmk@yahoo.co.uk>>
Sat, 03 Jun 2006 20:51:48 +0100

> ...understand the horrible collateral damage that their proposals would do.

Here in the UK (where plans for ID cards are well advanced), it's difficult to avoid the feeling that legislators and their backers ****do**** know that their proposals may well have undesirable side-effects, but they feel that these are worthwhile in the fight against child pornography, international terrorism, financial fraud, or whatever, and anyone who suggests caution (such as pointing out the RISKS of large-scale IT projects) and a more-considered approach is accused of wantonly obstructing

their efforts.

A cynic may feel that legislators are often inclined to brush objections aside just to show how tough they are being in dealing with serious problems, and as governments want to be seen to be doing something and people (voters) like to be reassured, intrusive but ineffective measures are favoured over effective but discreet ones. The deeper trouble seems to be modern politicians' liking for legislation as a fix for every problem; few people probably want to live in a country like 1970s East Germany, but some of us seem to be getting there anyway.

243,000 Hotels.com credit-card numbers stolen

<RsH <robert.heuman@alumni.monmouth.edu>>

Sat, 03 Jun 2006 10:07:29 -0400

CNNMoney reports that about 243,000 Hotels.com credit-card numbers were stolen back in February via the theft of a laptop computer. They believe that the theft was of the computer, with no idea of the information on the hard drive, and, likely as well, no intention of using the information on the hard drive. That it takes from February to June to determine what was on the hard drive is difficult to accept, however, and leaves unanswered what MIGHT have happened in the intervening three months respecting identity theft or misuse of the credit cards. Lots of unanswered questions, but

typical of the problem when a laptop gets stolen... [Source:
CNNMoney.com,
2 Jun 2006]

🔥 Data files erased at Aznar Government systems

<"Miguel A Gallardo O WWW.CITA.ES" <miguel@cita.es>>
Sun, 4 Jun 2006 11:20:36 +0200

Aznar Government deleted all the Spanish Government Presidency computer systems in "La Moncloa" Official Palace after the elections (3 days after the terrorism attacks in Madrid-Atocha train station). There is a 12 thousand Euros bill just for deleting everything, even data back-ups.

We are trying to find ways to ask for political and criminal responsibilities, and right now we need international cases, news, and references of official data deleted in government systems. As far as we know, in USA is not possible to do anything like that, and even Henry Kissinger files will be known in the years to come. I mean that USA presidents can encrypt and legally protect that information, but they can not erase as Aznar did.

You can find a lot of information (in Spanish) and our criminal accusation at <http://www.cita.es/borrado>

We expect expensive lawyers fees and a bail in order to keep the case alive in a Spanish Court of Law, so we need financial help and

international media
broadcasting. We found some support in archivists from several
Spanish
speaking countries already and I shall appreciate any help or
expert
witnessing support in order to explain to the judge how serious
is the case
documented at <http://www.cita.es/borrado>

Please do not hesitate to contact me for further information and
forward a
copy of this message to anyone you consider more appropriate.

Miguel A. Gallardo O., Engineer, Criminologist and Forensic
Cryptologist

President of APEDANICA at www.cita.es/apedanica

CV con fotos en <http://www.cita.es/conmigo>

Skype: m.a.g.o. Tel: (+34) 914743809 móvil 619776475

www.cita.es Apartado (P.O. Box) 17083-28080 Madrid, Spain

✉ Spam King Settles With Texas, Microsoft

<Monty Solomon <monty@roscom.com>>

Sun, 4 Jun 2006 11:06:13 -0400

Associated Press item, 3 Jun 2006

One of the world's most notorious spammers has settled lawsuits
with the

state of Texas and Microsoft Corp. that cost him at least \$1
million, took

away most of his assets and forced him to stop sending the
nuisance e-mails.

Ryan Pitylak, 24, who graduated from the University of Texas
last month, has

admitted sending 25 million e-mails every day at the height of
his spamming
operation in 2004.

<http://www.quote.com/home/news/story.asp?story=58948931>

⚡ Risks of formulaic sanitization

<Geoff Kuenning <geoff@cs.hmc.edu>>

04 Jun 2006 22:34:33 -0700

I just ordered copies of my free annual credit report from www.annualcreditreport.com. One of the new options is to hide the last 4 digits of your Social Security Number in the report output. That's mildly nice, in case the printed report falls into the wrong hands.

At least one of the three major credit-reporting companies who participate in the web site, Equifax, also hides details of account numbers by blanking the last four digits. Again, a nice touch: somebody who gets your report can't get a list of all your credit-card numbers.

Problem 1: most other credit-card handlers (e.g., Web vendors) blank all BUT the last four digits. I frequently get invoices and packing lists saying "card ending in 1234". So between one of those and the credit report, nothing is hidden.

Problem 2: I have some student loans with Sallie Mae. It turns out that their account numbers are formed by appending 3 digits to the end of the SSN. So despite Equifax's kind blocking of 4 digits of my SSN, in reality only 1 digit is hidden from anybody who acquires my copy of the report.

Needless to say, if I print the report it'll get shredded when I'm done with it, and my on-disk copy will be encrypted. But what about my non-security-savvy neighbor?

Geoff Kuenning geoff@cs.hmc.edu <http://www.cs.hmc.edu/~geoff/>

✈ Re: NASA's DART spacecraft smashes into satellite ([RISKS-24.29,30](#))

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>
Fri, 02 Jun 2006 10:31:08 +0200

PGN reported on the DART-satellite collision ([Risks-24.29](#)) and Robert Schaefer ([Risks-24.30](#)) noted that ITAR restrictions may have been a contributing cause. The incident took place on April 15, 2005, so the report comes a year later.

Frank Moring, Jr. reported extensively on the investigation in Aviation Week and Space Technology, May 22, 2006, pp37-8. An on-line report by Moring, freely available, may be found by searching www.aviationnow.com for the two words "DART morring". For those who like to paste pieces together, the URL is http://www.aviationnow.com/avnow/search/autosuggest.jsp?docid=600549&url=http%3A%2F%2Fwww.aviationnow.com%2Favnow%2Fnews%2Fchannel_space_story.jsp%3Fview%3Dstory%26id%3Dnews%2FITAR05176.xml

A U.K. firm, Surrey Satellite Technology Ltd., supplied the DART

prime

contractor Orbital Sciences Corp. with the primary GPS receiver used for the rendezvous manoeuvre. The GPS receiver registered a spacecraft velocity in error by about 0.6 m/sec. This led to a significant difference between estimated and measured positions, which led to the DART spacecraft resetting its position computations, with the biased data, which led through the same discrepancy to repeated resets, because the feedback "gain" was such that the estimated and measured positions could not have converged. "The anomaly caused excessive consumption of the spacecraft's ... fuel. It also led to the collision with the target satellite,..." (Morrison, Avweek op.cit. p37)

The bias in the Surrey GPS receiver was known, but the software fix for it had never been implemented by the DART team, and the bias was not reflected in the software model simulating the GPS receiver in preflight testing, so this simulation failed to elicit the reset problem, says the report (Morrison, op.cit, p37-8).

Morrison's article, and the report, also consider the human, organisational and developmental weaknesses and failures that led to this anomaly arising in operations. The redacted summary of the report says "In the case of DART, the MIB concluded that insufficient technical communication between the project and an international vendor due to perceived restrictions in export-control regulations did not allow for adequate insight" (op.cit., p.37). (I read this to mean restrictions *derived from* export-

control
regulations.)

Peter B. Ladkin, Causalis Limited and University of Bielefeld
www.causalis.com www.rvs.uni-bielefeld.de

Re: \$8 million for self-parking charge (Kuenning, [RISKS-24.30](#))

<Gabe Goldberg <gabe@gabegold.com>>
Sun, 04 Jun 2006 09:15:01 -0400

Geoff Kuenning reported an *LA Times* humor photograph featuring a self-pay parking kiosk with a mis-set date of 16 May 1943, showing an amount due of \$8,082,022.84.

And he commented, "Sanity checking, you ask? Not bloody likely. An auxiliary display shows the fee in larger characters; it reads 8.1E+6. When you have an programmer so clueless as to calculate money values in floating point, there is little hope for subtleties like sanity checking."

And continued, "As a side point, I'm fascinated that things like parking kiosks now use chips powerful enough to have floating-point support, at least as a library. A 4-bitter would be adequate for the task, though it's not clear to me that this particular programmer could have written the code needed to compute the fee on a 4-bit machine."

Assuming that the photo is genuine, it seems at least plausible that the programmer used a software library for calculating cost based on

elapsed
time rather than explicitly using floating point. Regarding the
chip's
bitness, unless the programmer is writing assembler code (risky
business for
such a mundane application), it seems unlikely that modern
programming
languages are supported by 4-biters.

Sanity check? Sure, programming insanity is easily detected in
hindsight. The kiosk should have refused a date earlier than
some epoch. But
what was the 1943 date? The kiosk's "current" date? The date a
car was
supposedly parked? The fee calculation might have refused to
present an
amount greater than some number. But what specs was the
programmer coding
from? What government agency requirements were the specs derived
from? Why
didn't a simple test case involve feeding the kiosk a
prehistoric date?

I guess the computer risk is debugging and proposing a solution
based on a
photograph of an incorrect result, not to mention blaming the
anonymous
programmer for (perhaps) just coding to design. And the
manufacturer for
using current technology vs. (perhaps) obscure and hard-to-
program
minimalist hardware.

Though, of course, there's likely a big-city market (New York,
certainly)
for parking meters displaying fees in floating point.

[Similar comments from Ray Blaak. PGN]

Re: Nationwide's Website Refuses Customer Feedback (Brady, [R-](#)

24.30)

<Michael Hogsett <michael.hogsett@sri.com>>

Thu, 01 Jun 2006 14:33:44 -0700

I get these all the time. All spam that is caught going to our mailing lists is forwarded to me and appropriately filed away automatically. I get about 3000 spam messages a day. I got 6 identical phishing emails for some bank today and forwarded one of the messages to both abuse@domain and security@domain. Those addresses often exist. I don't bother looking up addresses at their sites.

REVIEW: "Software Configuration Management Using Vesta", Heydon et al.

<"Rob, grandpa of Ryan, Trevor, Devon & Hannah" <rMslade@shaw.ca>>

Fri, 02 Jun 2006 08:42:05 -0800

BKSWCMUV.RVW 20060514

"Software Configuration Management Using Vesta", Allan Heydon et al.,

2006, 0-387-00229-4, U\$59.95

%A Allan Heydon

%A Roy Levin roy@Levin.net

%A Timothy Mann

%A Yuan Yu

%C 233 Spring St., New York, NY 10013

%D 2006

%G 0-387-00229-4

%I Springer-Verlag

%O U\$59.95 212-460-1500 800-777-4643 matthew.

giannotti@springer.com

%O <http://www.amazon.com/exec/obidos/ASIN/0387002294/>

[robsladesinterne](#)

<http://www.amazon.co.uk/exec/obidos/ASIN/0387002294/>

[robsladesinte-21](#)

%O <http://www.amazon.ca/exec/obidos/ASIN/0387002294/>

[robsladesin03-20](#)

%O Audience s Tech 3 Writing 1 (see revfaq.htm for explanation)

%P 262 p.

%T "Software Configuration Management Using Vesta"

The preface tells us that Vesta is a system for version and build control suitable for projects of all sizes, from the small, to those large and distributed to such an extent that the standard software management tools are inadequate.

Part one provides a general description of Vesta. Chapter one is an introduction, both to the common versioning (and related debugging and testing) problems, and to the principles of Vesta: versioning of source code and tools (with automated handling of relevant object code), "immortal" storage of all versions, and storage of complete system model descriptions of all builds and options used in compilation. ("Sources," in Vesta, are not limited to source code: tools introduced into the system are treated in similar ways. In addition, immortality is limited to source code: when a derived entity; one that is built or compiled; is unused for some period it may be weeded.) Various development related concepts from UNIX are listed in chapter two. The reason for this is not completely clear, but some of the ideas are used in chapter three, which describes Vesta at an abstract level.

Part two outlines the view of a Vesta user: the perspective of the programmer or developer. Chapter four reviews the management of versions and sources. The notion of a name space is similar to the UNIX file system or the Internet's domain name system (which it partially uses), with additional linking and restrictions on reuse. There is no specific support for merging of changes, in Vesta, but the tools can be modified to call for a merge utility from another source. Chapter five outlines the System Description Language (SDL), a scripting language for specifying "building" in Vesta. An example of the use of the language is given in chapter six.

Part three looks inside Vesta. Chapter seven examines internal operations of the repository. The Vesta evaluator is essentially responsible for compilation of the software project: chapter eight reviews the characteristics that allow it to manage complex development efficiently, reusing as much prior material as possible as the changes are made incrementally. The weeder attempts to deal with the issue of a system that can expand forever on a finite disk: the algorithms for making the balance between keeping too much (running out of space) and keeping too little (having to spend too much time recreating needed parts) are given in chapter nine.

Part four allows us to assess Vesta. Chapter ten reviews some competing systems: RCS (Revision Control System), CVS (Concurrent Versions System, Make, and a few CASE (Computer Aided Software Engineering) tools.

Performance, in terms of various speeds, memory loads, and storage requirements, are examined in chapter eleven. The data is, unfortunately, not from recent projects that used the system, but does show that Vesta convincingly outperforms Make, even for relatively small projects. (Suggestions are also given for enhancements to improve the system even further.) The conclusion, in chapter twelve, repeats much of the material in the preface.

An appendix provides a reference manual for the SDL. Vesta is available as an open-source tool at the www.vestasys.org Web site.

The authors admit, in chapter twelve, that there would be a learning curve involved in persuading developers to use the Vesta programming environment: Vesta does work in ways that would, initially, be mysterious to coders familiar with the currently popular tools. In addition, there would be some overhead involved in teaching programmers to use SDL. (On the other hand, new programmers would probably take to it quite readily.)

The book is intended as a research report rather than a user manual (although part two can be used to get started with the system). Much of the material concentrates on the internals of the system, and the aspects that assist in the excellent performance: these operations will never be seen by the user, although the system response will be satisfying. The authors have made no attempt to understand the information (and writing style) that would be helpful to developers attempting to use the system, and

managers trying
to decide whether or not to implement it. Open source devotees
wanting to
understand and extend the project will find this an invaluable
resource.

Researchers in the fields of software development and system
performance

will also find much of interest in these pages.

copyright Robert M. Slade, 2006 BKSWCUMV.RVW 20060514

rslade@vcn.bc.ca slade@victoria.tc.ca

rslade@computercrime.org

<http://victoria.tc.ca/techrev/rms.htm>

REVIEW: "Perfect Passwords", Mark Burnett

<"Rob, grandpa of Ryan, Trevor, Devon & Hannah" <rMslade@shaw.ca>>

Mon, 05 Jun 2006 10:57:41 -0800

BKPRFPWD.RVW 20060420

"Perfect Passwords", Mark Burnett, 2006, 1-59749-041-5,
U\$24.95/C\$34.95

%A Mark Burnett

%C 800 Hingham Street, Rockland, MA 02370

%D 2006

%G 1-59749-041-5

%I Syngress Media, Inc.

%O U\$24.95/C\$34.95 781-681-5151 fax: 781-681-3585 amy@syngress.
com

%O [http://www.amazon.com/exec/obidos/ASIN/1597490415/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/1597490415/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/1597490415/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/1597490415/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/1597490415/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/1597490415/robsladesin03-20)

%O Audience i- Tech 1 Writing 1 (see revfaq.htm for
explanation)

%P 181 p.

%T "Perfect Passwords: Selection, Protection, Authentication"

Those of us in the security field know that users are generally bad at creating passwords, and that passwords that are easily guessed or found account for huge numbers of security incidents. Therefore, I am in full sympathy with a book that attempts to lay out some guidance on password choice. However, Burnett's work calls to mind the old joke that lists all kinds of restrictions on password selection, and finally admits that only one possible password actually fits the criteria, and will all users please contact tech support to be issued with that password.

Chapter one tells us that people choose weak passwords, and gives a number of lists of such poor choices, without an awful lot of explanation. (Burnett also states that the choice of strong passwords provides non-repudiation, which is a rather strange position. One could make a case that the deliberate choice of a vulnerable password would allow the user to later claim that their account had been hacked, and therefore assist with repudiation, but the reverse doesn't necessarily hold.) Various types of password cracking techniques are given in chapter two. This begins to show the inconsistencies and contradictions that plague the text: at one point we are told that any password less than fifteen characters is "immediately" available to attackers, but elsewhere it is suggested that a ten character password is a wise choice. (Although brute force cracking is discussed extensively, there is, oddly, no mention of the implications of Moore's Law.) There is a good discussion of the vital issue of

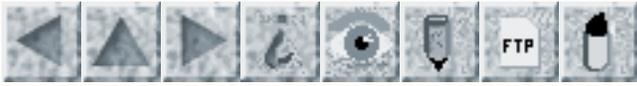
randomness in chapter three, although there are numerous gaps, and, again, erratic suggestions. Chapter four covers character sets and address space. Unfortunately, it is rather impractical (as are other areas of the manual) due to a lack of recognition of character restrictions. Password length is addressed in chapter five, covering many of the same concepts as in four. It is also the most useful of the material to this point in the book, suggesting ways to lengthen and harden passwords already chosen and preferred. (Some of the advice is suspect: bracketing is easy to add to automated password cracking programs, and even Burnett admits that "colorization" is a weak idea due to the limitations on selection.) Chapter six takes an extremely terse and abbreviated look at password aging, but all that is really said is that it is inconvenient. Miscellaneous advice about using, remembering, storing, and managing passwords is given in chapter seven. Chapter eight provides password creations tips, but these are, after some of the previous material in the book, rather weak, and typically boil down to the use of passphrases and long passwords. Five hundred weak passwords are listed in chapter nine, but the purpose of the list is not clear. As with chapter one, the passwords are not analysed for strength in any way, and, even if you want to check your favourite against the list, it isn't in alphabetical order. Additional password creation tips are in chapter ten, these slightly more useful. We are told, in chapter eleven, to make complex passwords, uncommon passwords, and not to tell anyone our

passwords. Chapter twelve suggests having a regular "password day" set aside to concentrate on changing passwords and creating strong ones. Other forms of authentication are discussed in chapter thirteen.

While the advice and information given in the book is not bad, it seems to posit a fairly ideal world. A number of practical items can assist users with password choice, but a number of realistic considerations are ignored. Readers may also be confused by the lack of constancy in the recommendations. Certainly the structure of the text could use work: concepts are repeated in different chapters, and the advice seems to be aggregated and presented at random.

There is good advice in this manual, but it lacks focus. The average computer user would probably receive a lot of benefit, but is unlikely to purchase or read anything this size on this topic. (A pocket sized volume, along the lines of the O'Reilly "Desktop Reference" series would be ideal.) System administrators would be able to understand and use the material in the book, although much of the content is either known or available. On balance, I would recommend that this primer is important, but definitely needs work.

copyright Robert M. Slade, 2006 BKPRFPWD.RVW 20060420
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<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

Search RISKS using [swish-e](#)

Volume 24: Issue 32

Wednesday 14 June 2006

Contents

- [Hospitals have dramatically reduced unnecessary deaths](#)
[PGN](#)
- [Unverified air traffic data](#)
[David Magda](#)
- [Report on security risks of applying CALEA to VoIP](#)
[Susan Landau](#)
- [TIAA Breaches Whistleblower](#)
[Al Macintyre](#)
- [Cybersecurity plan of the Federal government: what a screw-up](#)
[Fred Cohen](#)
- [IRS Laptop Lost With Data on 291 People](#)
[Christopher Lee via Monty Solomon](#)
- [Windows XP update may be classified as "spyware"](#)
[Lauren Weinstein](#)
- [How MS spyware could be used by hackers to disable systems](#)
[?](#)
- [DoE Discloses Data Theft](#)
[Ari Ollikainen via Dave Farber](#)

- [UnSalted Credit Cards](#)
[Mark Ennis](#)
 - [Lottery scam spam -- unclear on the concept](#)
[Drew Dean](#)
 - [Dental X-Rays go Digital---same old problems](#)
[Howard Israel](#)
 - [Silver Bullet: Dan Geer](#)
[Gary McGraw](#)
 - [REVIEW: "Software Security: Building Security In", Gary McGraw](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Hospitals have dramatically reduced unnecessary deaths

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

Wed, 14 Jun 2006 12:25:59 PDT

[Do you recall "Hospital operates on wrong patient?" (lead item in

[RISKS-24.11](#))? This is the other side of the coin. TNX to Lauren

Weinstein for sending this one to me. PGN]

Hospitals Cut Lethal Errors Rate, Mike Stobbe, AP item, *Newsday*, 14 Jun 2006

<http://www.newsday.com/news/nationworld/wire/sns-ap-hospital-lifesavers,0,6425411.story?coll=sns-ap-nationworld-headlines>

A campaign to reduce lethal errors and unnecessary deaths in U. S. hospitals

has saved an estimated 122,300 lives in the last 18 months.

About 3,100

hospitals participated in the project, sharing mortality data and carrying

out study-tested procedures that prevent infections and mistakes. Experts

say the cooperative effort was unusual for a competitive

industry that traditionally doesn't like to publicly focus on patient-killing problems. Medical mistakes were the focus of a widely noted 1999 national report that estimated 44,000 to 98,000 Americans die each year as a result of errors and low-quality care.

Perhaps the best known of the six changes was to deploy rapid response teams for emergency care of patients whose vital signs suddenly deteriorate. ... Another urged checks and rechecks of patient medications to protect against drug errors. A third focused on preventing surgical site infections by following certain guidelines, including giving patients antibiotics before their operations.

Unverified air traffic data

<David Magda <dmagda@ee.ryerson.ca>>
Thu, 8 Jun 2006 19:19:39 -0400

Dick Smith [1] is warning [2] that the new ADS-B air traffic system [3] uses unverified data to plot what (supposedly real) aircraft are doing:

> But Mr Smith, who is campaigning against the scheme and has raised safety
> and security concerns about the design, said the system had no way of
> verifying whether a plane was where it claimed to be or if it existed at
> all.
>

> He said the FAA was looking at ways of encrypting signals or setting up
> multiple ground stations at each location to allow the traffic controllers
> to determine whether a signal came from a moving aircraft.

The main advantage of the system is that radar (which is expensive to buy and run) is not needed since aircraft broadcast their (supposed) position, and that data can be received using less expensive equipment. Aircraft determine their position by GPS.

I'm sure the disadvantages of an unauthenticated positioning system don't have to be spelled out.

[1] http://en.wikipedia.org/wiki/Dick_Smith

[2] <http://www.theaustralian.news.com.au/story/0,20867,19378061-23349,00.html>

[3] http://en.wikipedia.org/wiki/Automatic_Dependent_Surveillance-Broadcast

Report on security risks of applying CALEA to VoIP

<Susan Landau <susan.landau@sun.com>>

Tue, 13 Jun 2006 15:29:56 -0400

Below you'll find an executive summary of "Security Implications of Applying the Communications Assistance for Law Enforcement Act to Voice over IP."

The full report is at <http://www.itaa.org/news/docs/CALEAVOIPreport.pdf> .

Security Implications of Applying the Communications Assistance to Law

Enforcement Act to Voice over IP

Steven Bellovin, Columbia University
Matt Blaze, University of Pennsylvania
Ernest Brickell, Intel Corporation
Clinton Brooks, NSA (retired)
Vinton Cerf, Google
Whitfield Diffie, Sun Microsystems
Susan Landau, Sun Microsystems
Jon Peterson, NeuStar
John Treichler, Applied Signal Technology

Executive Summary

For many people, Voice over Internet Protocol (VoIP) looks like a nimble way of using a computer to make phone calls. Download the software, pick an identifier and then wherever there is an Internet connection, you can make a phone call. From this perspective, it makes perfect sense that anything that can be done with a telephone, including the graceful accommodation of wiretapping, should be able to be done readily with VoIP as well.

The FCC has issued an order for all ``interconnected'' and all broadband access VoIP services to comply with Communications Assistance for Law Enforcement Act (CALEA) --- without specific regulations on what compliance would mean. The FBI has suggested that CALEA should apply to all forms of VoIP, regardless of the technology involved in the VoIP implementation.

Intercept against a VoIP call made from a fixed location with a fixed IP address directly to a big Internet provider's access router is equivalent to wiretapping a normal phone call, and classical PSTN-style CALEA concepts can

be applied directly. In fact, these intercept capabilities can be exactly the same in the VoIP case if the ISP properly secures its infrastructure and wiretap control process as the PSTN's central offices are assumed to do.

However, the network architectures of the Internet and the Public Switched Telephone Network (PSTN) are substantially different, and these differences lead to security risks in applying the CALEA to VoIP. VoIP, like most Internet communications, are communications for a mobile environment. The feasibility of applying CALEA to more decentralized VoIP services is quite problematic. Neither the manageability of such a wiretapping regime nor whether it can be made secure against subversion seem clear. The real danger is that a CALEA-type regimen is likely to introduce serious vulnerabilities through its ``architected security breach.''

Potential problems include the difficulty of determining where the traffic is coming from (the VoIP provider enables the connection but may not provide the services for the actual conversation), the difficulty of ensuring safe transport of the signals to the law-enforcement facility, the risk of introducing new vulnerabilities into Internet communications, and the difficulty of ensuring proper minimization. VOIP implementations vary substantially across the Internet making it impossible to implement CALEA uniformly. Mobility and the ease of creating new identities on the Internet exacerbate the problem.

Building a comprehensive VoIP intercept capability into the Internet appears to require the cooperation of a very large portion of the routing infrastructure, and the fact that packets are carrying voice is largely irrelevant. Indeed, most of the provisions of the wiretap law do not distinguish among different types of electronic communications. Currently the FBI is focused on applying CALEA's design mandates to VoIP, but there is nothing in wiretapping law that would argue against the extension of intercept design mandates to all types of Internet communications. Indeed, the changes necessary to meet CALEA requirements for VoIP would likely have to be implemented in a way that covered all forms of Internet communication.

In order to extend authorized interception much beyond the easy scenario, it is necessary either to eliminate the flexibility that Internet communications allow, or else introduce serious security risks to domestic VoIP implementations. The former would have significant negative effects on U.S. ability to innovate, while the latter is simply dangerous. The current FBI and FCC direction on CALEA applied to VoIP carries great risks.

TIAA Breaches Whistleblower

<Al Macintyre <macwheel99@sigeom.net>>

Sat, 10 Jun 2006 21:49:41 -0500

go.eweek.com/tiaa

IT Manager seeks redress for firing, claiming SARBOX
Whistleblower protection

<http://www.eweek.com/article2/0,1759,1969518,00.asp>

US Supreme Court lowers Whistleblower protection for employees
reporting

fraud or criminal misconduct to the proper authorities, but
employees have

more protection if they go straight to the news media

[http://www.accountingweb.com/cgi-bin/item.cgi?](http://www.accountingweb.com/cgi-bin/item.cgi?id=102230&d=815&h=817&f=816&dateformat=%25B%20%25e,%20%25Y)

[id=102230&d=815&h=817&f=816&dateformat=%25B%20%25e,%20%25Y](http://www.accountingweb.com/cgi-bin/item.cgi?id=102230&d=815&h=817&f=816&dateformat=%25B%20%25e,%20%25Y)

[http://www.forbes.com/technology/feeds/ap/2006/05/30/ap2780736.
html](http://www.forbes.com/technology/feeds/ap/2006/05/30/ap2780736.html)

<http://civilliberty.about.com/b/a/257515.htm>

This is a familiar and disturbing picture. Personnel find
security problems
with employer systems, report them, nothing happens. Computer
staff exhaust
what can be done in-house to get the security problems resolved,
but
leadership resistance is too strong.

A year later there is a serious security breach. Top Managers
claim nothing
much at risk, but ask computer staff to help the feds find out
exactly what
was breached, which turns out to be practically everything.
Computer staff
gets fired.

What makes this worse is the news that the Feds apparently
support the
coverup, when the whistleblowers appeal the employer punitive
action.

Had computer staff lied to investigators, claiming no problem,
like
management had wanted, they would still have their jobs.

Thus computer workers have to balance behavior that will help career integrity vs. what is in the best interests of protecting customers and investors.

However, there are lots of news stories of whistleblowers who successfully prevail, so we should wait and see what happens in this case.

🔥 Cybersecurity plan of the Federal government: what a screw-up

<Fred Cohen <dr.cohen@mac.com>>

Thu, 8 Jun 2006 06:01:35 -0700

I just read the new plan for funding information security at the Federal level and it was pathetic. The most notable element of it is the fact that they claim to align between several different things but in fact they don't align at all. The things they identify as worth doing are the very things that don't need to be done and the things they identify as not worth doing are the things we most desperately need. But fear not - they won't put any real money behind anything worthwhile in any case. The plan - if fully implemented - would not even stop the large-scale theft of identity information of all the people getting clearances or all the folks in the military. So we won't be getting much in the way of help from the federal government in advancing the field for the next few years at least.

www.nitrd.gov/pubs/csia/csia_federal_plan.pdf

Fred Cohen & Associates; Security Posture; University of New Haven; ASP Press
all.net, securityposture.com, unhca.com, asp-press.com, 1-925-454-0171

IRS Laptop Lost With Data on 291 People

<Monty Solomon <monty@roscom.com>>

Sun, 11 Jun 2006 21:13:33 -0400

An Internal Revenue Service employee lost an agency laptop early last month that contained sensitive personal information on 291 workers and job applicants, a spokesman said yesterday.

The IRS's Terry L. Lemons said the employee checked the laptop as luggage aboard a commercial flight while traveling to a job fair and never saw it again. The computer contained unencrypted names, birth dates, Social Security numbers and fingerprints of the employees and applicants, Lemons said. Slightly more than 100 of the people affected were IRS employees, he said. No tax return information was in the laptop, he said. "The data was not encrypted, but it was protected by a double-password system," Lemons said. "To get in to this personal data on there, you would have to have two separate passwords." Lemons said the Treasury Department's inspector general for tax administration is investigating the loss. The IRS is notifying affected individuals and advising them on steps to

guard against
identity theft. Lemons declined to name the airline or the
employee, or to
say whether the worker was disciplined, citing the ongoing
investigation.

... [Source: Christopher Lee, *The Washington Post*, 8 Jun2006,
A04; PGN-ed]

[http://www.washingtonpost.com/wp-dyn/content/article/2006/06/07/
AR2006060701987.html](http://www.washingtonpost.com/wp-dyn/content/article/2006/06/07/AR2006060701987.html)

Windows XP update may be classified as "spyware" (from Farber's IP)

<Lauren Weinstein>

June 6, 2006 1:15:05 AM EDT

There have been some murmurs about this in other forums, but
since I've now
independently verified I figured I'd better report here.

A recent Microsoft update to Windows XP, which modifies the tool
that
verifies the "validity" of XP installations to ensure that they
are not
illicit, may itself be considered to be spyware under commonly
accepted
definitions.

The new version of the "Microsoft Genuine Advantage" tool
reportedly will
repeatedly nag users of systems it declares to be invalid, and
will then
apparently deny such users various "non-critical" updates.
Apparently
various parties have already found ways to bypass this tool,
though the
effects of this on later updating capabilities remain to be seen.

However, I've noted a much more serious issue on local XP systems, all of which are legit and pass the MS validity tests with flying colors. It appears that even on such systems, the MS tool will now attempt to contact Microsoft over the Internet *every time you boot*. At least, I'm seeing these contacts on every boot after the tool update so far, and I've allowed them to proceed to completion each time. Perhaps it stops after some number of boots, but there's no indication of such a limit so far. The connections occur even if you do not have Windows "automatic update" enabled. ...

<http://www.interesting-people.org/archives/interesting-people/200606/msg00030.html>

⚡ How MS spyware could be used by hackers to disable systems

<(?)>

Mon, 12 Jun 2006 12:11:53 -0700 (PDT)

An anonymous Slashdot user gives virus writers a worrying idea: "A virus could use one of the 'Product-Key Changer' scripts ... to install a pirated product key on every infected computer (wiping all traces of the original key). This would render millions of genuine installations indistinguishable from pirated installations. What a mess for Microsoft! They would have to immediately 'kill forever' the WGA helper, and maybe even remove the WGA

check on Windows Update. Such a virus would be a hard lesson to learn for the writers of all kinds of automated 'genuine' checks."

⚡ DoE Discloses Data Theft (via Dave Farber's IP)

<Ari Ollikainen <Ari@OLTECO.com>>
June 10, 2006 1:37:31 PM EDT

Foot dragging on an incident which occurred in September 2005...
[and was not reported until 8 June 2006. PGN]

Energy Dept. Discloses Data Theft
Victims, Top Officials Were Not Told About 2005 Hacking

A hacker stole a file containing the names and Social Security numbers of 1,500 people working for the Energy Department's nuclear weapons agency.

[Source: Associated Press item, *The Washington Post*, 10 Jun 2006, A04]

<http://www.washingtonpost.com/wp-dyn/content/article/2006/06/09/AR2006060901505.html>

⚡ UnSalted Credit Cards

<Mark Ennis <mark@netcommute.ie>>
Tue, 13 Jun 2006 15:14:25 +0100 (BST)

The credit card companies publish what is colloquially known as the PCI standard. For the standard itself, see:

http://usa.visa.com/download/business/accepting_visa/

[ops_risk_management/cisp_PCI_Data_Security_Standard.pdf](#)

This covers various aspects of security for organisations that are involved in the processing of credit cards.

I'm surprised to see however that where they suggest that cardholder data is secured:

Render sensitive cardholder data unreadable anywhere it is stored (including data on portable media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches.

- One-way hashes (hashed indexes), such as SHA-1
- Truncation
- Index tokens and PADs, with the PADs being securely stored
- Strong cryptography, such as Triple-DES 128-bit or AES 256-bit with associated key management processes and procedures.

They omit to mention that one-way hashes of cardholder data are of little use without applying a salt. They should - as has been documented here before many programmers see no problem in wrapping a bare md5 function around a sensitive value.

For instance - as is well known 16 digit credit card numbers start with a 6 digit bank code and end with a checksum. A reverse hash dictionary for all unsalted MD5 codes for one bank code only needs to cover $16 - 6 - 1 = 9$ digits of possibilities - or one thousand million entries. This could be done for a storage cost of:

9 digit number = 4 bytes
MD5 checksum = 16 bytes number
Total = 20 bytes * 1,000,000,000 possibilites = 20Gb

As a result its completely feasible a program that asks for unsalted MD5 or SHA-1 Hash of a credit card number and the 6 digit bank code could generate the original credit card number after waiting for that bank code's 20gb dictionary to be generated.

Mark Ennis, NetCommute Ltd. <mark@netcommute.ie> 00-353-1-8569539

⚡ Lottery scam spam -- unclear on the concept

<Drew Dean <ddean@CS.Princeton.EDU>>
Wed, 7 Jun 2006 08:51:16 -0700

In my Inbox:

> CONGRATULATIONS: YOU WON -1,000,000.00 EUROS.

I'm sure they'd like me to give them 1 million Euros, but I think not. With my permission, they'll even enter me into a drawing for -5 Million Euros!
Wow, my lucky day! :-)

⚡ Dental X-Rays go Digital---same old problems

<h.israel@comcast.net>
Wed, 07 Jun 2006 18:25:28 +0000

Personal experience, with my dentist yesterday evening.

It was a typical visit, except now my dentist is using a new digital x-ray machine (from Kodak) that runs on a standard PC (probably this system:

<http://www.kodak.com/global/en/health/dental/documentation/sysReqs/KDIS.pdf>

).

The process to take the X-Ray is relatively the same as the old analog method. Noticeable differences: 1) the X-Ray machine is physically smaller, 2) there is no film, but in its place is a reusable digital sensor with a trailing wire leading out of the patients mouth. 3) images are rendered immediately on a screen, so the tech can determine if the shot taken is OK or needs to be re-taken. 4) the images are very clear and noticeably sharper than the analog X-Rays (to my untrained eye).

Now the not so fun part. After the tech completes the set of 6 pictures, the dentist comes in to review. A few clicks and pop ups appear, a few too quick clicks, and poof, the images are accidentally deleted and not retrievable. The tech admitted afterward that she usually does a save before the dentist comes in. OK, lets do it again. Take a second set of images. The tech does the save, but an hour glass comes up and the PC freezes. The images are mostly still visible on the screen, except there are a couple of pop-ups that are blocking one of the images of my teeth and they can not be moved. The dentist comes in to review the images, but can not

access the application, since it is not functioning. The obvious thing to do is a CTL-ALT-DEL to see what is going on. The CPU is idle, but the app is "not responding". The dentist claims that this is the first problem he has had in the few months he has been using the system. Since most of the images are actually still viewable, he does his assessment, then starts to end the hung processes.

Eventually a "Send Error Report" window appears giving the user the option to send in an error report to the software maker, which he elects not to send. He reboots, then brings up the application, and then tries to access my patient record and see if the X-Ray images were actually saved, but the app gives him an error. My guess is that a file corruption occurred.

Of Note: The PC is Internet enabled, via dial-up access. I believe it is used to transmit data for insurance processing (as confirmed via link below). Aside from the obvious application issues described above, I started to wonder about HIPAA issues and how well my data/info is protected by this PC linked to the Internet. Also, thinking about what backup systems are in use, etc. Another thought--how easy would it be to manipulate the digital images to sabotage a forensics investigation (another great use of PhotoShop!)? Delete the images to prevent the positive ID of a body, or better yet, cause a body to be incorrectly identified (e.g., fake ones death). Do these images have digital signatures? (Doubt it!)

While I didn't dig into it deeply, its just a matter of time before ...

Here is a link to an online article (WSJ reprint?): <http://www.mindfully.org/Technology/2005/Dental-X-Ray-Digital29nov05.htm>

It highlights some pros/cons of going digital.

Howard Israel, CEO, Secure Systems Consulting, LLC 1-732-613-9464

🔥 Silver Bullet: Dan Geer

<"Gary McGraw" <gem@cigital.com>>

Mon, 12 Jun 2006 13:35:29 -0400

The second edition of the Silver Bullet Security Podcast with Gary McGraw

(hey, that's me) went up just a few seconds ago:

<http://www.cigital.com/silverbullet/>

The first show (with Avi Rubin) proved to be pretty popular.

Hope you all

like this one too! Feedback welcome through the website.

Marcus Ranum is on deck and Dana Epp is on the list. Who else do you want

to hear from in Silver Bullet?

gem www.cigital.com www.swsec.com

🔥 REVIEW: "Software Security: Building Security In", Gary McGraw

<Rob Slade <rMslade@shaw.ca>>

Mon, 12 Jun 2006 11:54:22 -0800

BKSWBSI.RVW 20060518

"Software Security: Building Security In", Gary McGraw, 2006,
0-321-35670-5, U\$49.99/C\$66.99

%A Gary McGraw swsec.com www.buildingsecurityin.com
gem@digital.com

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8

%D 2006

%G 0-321-35670-5

%I Addison-Wesley Publishing Co.

%O U\$49.99/C\$66.99 416-447-5101 800-822-6339 bkexpress@aw.com

%O [http://www.amazon.com/exec/obidos/ASIN/0321356705/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0321356705/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/0321356705/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0321356705/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/0321356705/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0321356705/robsladesin03-20)

%O Audience a+ Tech 3 Writing 2 (see revfaq.htm for
explanation)

%P 408 p. + CD-ROM

%T "Software Security: Building Security In"

The preface states that the audience for the book is comprised of developers (particularly those interested in secure software), security professionals (in places), managers (in places), and academics (there are a couple of chapters that indicate where further research might be useful). McGraw also introduces the major components of the book. His "three pillars" are not the usual confidentiality, integrity and availability, but risk management, "touchpoints," and knowledge. The touchpoints are code analysis, risk analysis, penetration (vulnerability) testing, security tests, abuse cases, security requirements, and security operations.

Part one outlines the basics of software security. Chapter one

informs us that problems exist in software, and notes the differences between bugs (due to careless implementation) and flaws (due to poor design). McGraw also suggests his three pillars as a means of addressing the difficulty. Using an example software project, chapter two takes us through a risk management framework in some detail.

Part two examines the touchpoints. Chapter three introduces them in a diagram related to the steps in the software development process (they are numbered, although in a seemingly random pattern which turns out to be the suggested order of effectiveness). (The latter half of the chapter seems to be more of a sermon on software security.) Source code review tools (for finding bugs) are described in chapter four. Chapter five starts off with traditional risk analysis definitions and then extends the concept with details of the application of the process to software design. (Sidebars on software tools for program risk analysis, and other related items, are dropped in seemingly at random. The information is valuable, but the reading flow is somewhat disjointed.) Penetration testing of software sounds like a good idea, but chapter six doesn't really define what the topic involves. (The sidebar on tools is a case in point: the tools are listed and recommended, but the descriptions don't say what they actually do.) Risk-based security testing seems, by the end of chapter seven, to be a special case of spanning tree analysis, but along the way a number of the

other touchpoints seem to overlap with it. "Abuse cases" is the application of known common vulnerabilities and attacks (perpetrated on systems similar to yours), and analysis of means of protection while still in the design phase. Chapter eight provides a handy list of such attacks (if you are building a Web application). "Security operations," in chapter nine, appears to be a discussion of how software developers and security professionals should relate to each other. (Touchpoint six, "security requirements," is not covered.)

Part three covers additional topics. Chapter ten outlines advice for a software security program in a large company. "Knowledge for software security," in chapter eleven, is mostly an overview of material already covered, but does include some additional tools. Chapter twelve is a taxonomy of coding errors, which should be valuable both for those working on analysis of their own program security, and also researchers in the field.

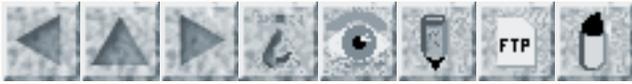
One fairly consistent weakness is that the book seems to assume that all software applications are network-based, and that all software problems result from malicious attacks. While Web-based applications are definitely of great importance, and also subject to a larger range of difficulties, this does limit the application of some of the material of the text in regard to standalone programs where the major concern is integrity of data, prevention of errors, and reliability of operation.

The writing and structure could use some work: in many situations it is not easy to follow the thread of McGraw's argument. However, there is no denying the value of having all these ideas about software security brought together in one volume. There is a great deal of useful and interesting material here, and, with commitment from the reader, much that will be helpful in building more robust and reliable software.

copyright Robert M. Slade, 2006 BKSWSBSI.RVW 20060518
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<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

Search RISKS using [swish-e](#)

Volume 24: Issue 33

Tuesday 20 June 2006

Contents

- [Backward switches: Genesis slammed to Earth after parachutes failed](#)
[Howard Israel](#)
- [Sunken Ferry Crew didn't know how to use ECS display software](#)
[Kelly Bert Manning](#)
- [Possible Loss of Space Shuttle: 'I think, at that point, we're done'](#)
[Harry Crowther](#)
- [More BART woes: automated train-control system mothballed](#)
[PGN](#)
- [German Federal Civil Court ruling on Robodoc cases](#)
[Juergen Fenn](#)
- [NZ IRD Numbers about to run out](#)
[M. Hackett](#)
- [Fortune cookie bet made Powerball lottery players rich](#)
[Howard Israel](#)
- [Wily crows disconnect wired Tokyo](#)
[PGN](#)
- [Another risk of electromagnetic interference](#)
[Tom Philp](#)

- [Volvo's self braking car](#)
[David Magda](#)
 - [Risks of Ajax and Javascript](#)
[Charlie Wertz](#)
 - [Ironic risk of using a 'free' mail service](#)
[Mike Scott](#)
 - [DoE Discloses Data Theft](#)
[Ari Ollikainen](#)
 - [Testing stolen credit card numbers](#)
[Walt Daniels](#)
 - [RFID "Best Practices"](#)
[CDT via Monty Solomon](#)
 - [Bank's redirector helps phishing](#)
[Fred Bone](#)
 - [Microsoft Patches crash IBM Midrange Consoles](#)
[Al Macintyre](#)
 - [Re: Man Gets \\$218 Trillion Phone Bill](#)
[Nancy Bogart](#)
 - [Re: Hospitals have dramatically reduced unnecessary deaths](#)
[Peter R Cook](#)
 - [Cyberwar](#)
[PGN](#)
 - [REVIEW: "Information Security and Employee Behaviour", McIlwraith](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Backward switches: Genesis slammed to Earth after parachutes failed

<"H Israel" <h.israel@comcast.net>>

Wed, 14 Jun 2006 21:27:19 -0400

Select relevant quotes from

<http://www.cnn.com/2006/TECH/space/06/14/genesis.crash.ap/index.html>

The 231-page document prepared by independent investigators found that gravity switches on the Genesis probe designed to trigger the deployment of its parachutes were installed backward.

Investigators found that the probe's builder, Lockheed Martin, skipped a critical pre-launch test that would have uncovered the fatal flaw because of time constraints. Instead, engineers decided to do a simpler test by comparing Genesis' design to drawings of another spacecraft, Stardust, which was built earlier and had passed rigorous testing.

The report also said lack of oversight by NASA's Jet Propulsion Laboratory, which managed the \$264 million mission, caused the error to remain undetected from the design phase to the review stage.

Investigators also faulted the space agency's "faster, better, cheaper" philosophy for creating an environment where cost issues were put ahead of a successful mission.

That philosophy "created an ever-present threat of cancellation if overruns occurred on cost-capped missions," investigators wrote. ...

And this quote, which appear to be conflicting 'requirements': "Clearly, we want missions to be cost-effective, but we don't want to cut corners just to make them cheaper," Jones said.

They probably meant to say something like this: "We want the missions to be successful, at the least cost possible." A laudable goal, not quite achievable with current technology, in my opinion.

Howard Israel, CEO, Secure Systems Consulting, LLC (732) 613-9464

✦ Sunken Ferry Crew didn't know how to use ECS display software

<bo774@freenet.carleton.ca (Kelly Bert Manning)>

Thu, 15 Jun 2006 11:47:51 -0400 (EDT)

Preliminary reports from the Canadian Transportation Safety board investigation into the "Queen of The North" running into Mount Gil and sinking say that the bridge crew had the Electronic Chart System Display turned off because they didn't know how to use the software control to reduce the illumination for night use.

The preliminary reports also say that bridge crew claim to not be fully aware of how to use the various steering modes, or even to know what steering mode they were in.

Digital controls should help, not hinder.

"The screen from the ECS produced too much ambient light, so the crew

would often turn it off at night, Ayeko wrote. The monitor would be

turned on momentarily only when it was required."

http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20060605/BC_ferry_060605/20060606?hub=Canada

This must have been an expensive system. Would it have been too much trouble to add a rotating dial or rocker button which would reduce or increase the brightness on the display? It wouldn't even have to be integrated with the monitor, just mounted somewhere close to it and clearly labeled. These don't

even need to be rheostatic controls, just something that generates an input specifying the type of change requested.

Software control is bad if it makes essential functions too complex or obscure.

Some reports describe Mt. Gil as Gil Island. It is a relatively tall and steep mountain whose base is underwater. There should have been a good radar return from it. It will be interesting to see what other electronic or computer integrated safety systems also failed to make the officer and helmsman aware that their failure to change heading at the scheduled time had left them on a collision course with a mountain.

It will also be interesting to see whether the ECS brightness control issue is a "reasonable doubt" red herring raised as a defense for the criminal trial which will take place. Two passengers are missing and presumed drowned.

✶ Possible Loss of Space Shuttle: 'I think, at that point, we're done'

<"Harry Crowther" <hdcrowther@alum.rpi.com>>

Mon, 19 Jun 2006 06:42:22 -0400

After a "spirited discussion"', space shuttle mission Discovery (STS-121) is scheduled to launch 'despite the reservations of two senior officials': the lead safety official & the chief engineer, over issues that "remained about

debris from the shuttle's external fuel tank that could damage the vehicle during launching.'

"If a shuttle is critically damaged during launching, (NASA administrator Michael) Griffin said, the crew could make it to the space station to await rescue by another shuttle or a Russian spacecraft. Such an accident would not unduly threaten crew safety, he said, but it probably would end the shuttle program. I would be moving to shut the program down," he said of the loss of another shuttle. "I think, at that point, we're done."

'rescue by another shuttle' would be the (then) sole remaining shuttle.

Why bother to ground it, under the circumstances?

[Source: Warren E. Leary, NASA to Launch Discovery on July 1 for 13-Day Mission, *The New York Times*, 18 Jun 2006]

✈ More BART woes: automated train-control system mothballed

<"Peter G. Neumann" <neumann@csl.sri.com>>
Sun, 18 Jun 2006 12:36:17 PDT

RISKS has long documented problems with the San Francisco Bay Area Rapid Transit system. The latest is that \$80 million have been spent on a long-planned automated train-control system that would enable a 25% increase in the number of trains that could go through the Transbay Tube. \$40M for equipment, \$40M for staff time. The effort is now on "indefinite hold".

Involved in a contract that began in 1998, Harmon Industries was acquired by GE Transportation Systems Global Signaling, a GE subsidiary, which BART officials claim has refused to honor the contract and GE claims is false.

The system was originally scheduled to be fully operational in 2004.

[Source: Rachel Gordon, BART: Transbay speedup on hold, *San Francisco

Chronicle*, 17 Jun 2006, B1,B7; PGN-ed] <http://www.sfgate.com>

German Federal Civil Court ruling on Robodoc cases

<Juergen Fenn <juergen.fenn@GMX.DE>>

Thu, 15 Jun 2006 02:28:02 +0200

In September 2003, I reported on "The benefits and risks of robot surgery"

using "Robodoc", a computer-controlled robot for hip and knee joint

implants, in use at a rather well-reputed German clinic at Frankfurt/Main.

The new method of medical treatment which was used since the mid-1990s in

Germany promised to be more precise than surgery done manually.

<http://catless.ncl.ac.uk/Risks/22.90.html#subj13>

Operations with Robodoc were suspended in this country since 2004 and the

senior surgeon using the robot had left the said clinic in 2005 already.

The first of the lawsuits pending ever since has now been decided, resulting

in the German Federal Civil Court, or Bundesgerichtshof, at Karlsruhe

declining any legal claims raised by a former patient against

either the clinic or the physicians using the robot for the operations at the time. The court thus upheld the earlier decisions by other German courts.

The court said in the ruling that patients must be told by physicians about the risks of new operating methods before undergoing surgery so that they can themselves decide whether they are willing to take risks hitherto unknown due to the small number of cases the all-new method was used in or whether he wants to be treated in a conventional way, i.e., in this case, by a surgeon without the help of a robot. However, in the case decided on June 13, 2006 the risk of damage to the patients' nerves about 11 years ago was the same as with conventional methods of operation she was told about before undergoing treatment. This is why the plaintiff who is now 49 years old was not eligible to compensation damages in this case which is the first in a series of rulings.

The press release on the decision (in German) can be found at:
<http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2006&Sort=3&nr=36501&anz=90&pos=0&Blank=1>

NZ IRD Numbers about to run out

<"M. Hackett" <dist23@juno.com>>
Mon, 19 Jun 2006 03:35:25 -0700

It seems as if NZ is taking a Canadian-style solution to its tax

number

length. However, the risks of going to the longer format are (really) not

known at this time. NZ has done a lot of background work with respect to

modernizing its government computer systems -- but IRD numbers span the

public and private sector. Australian, British, Canadian and Irish IT

systems relating to taxation and benefits that explicitly use the NZ IRD

number may also be affected.

[Source: Inland Revenue and GST number range is to be extended]

<https://www.ird.govt.nz/gst/gst-didyouknow.html>

Max Power, CEO, Power Broadcasting (PTY) <http://HireMe.geek.nz/>

🔥 Fortune cookie bet made Powerball lottery players rich

<h.israel@comcast.net>

Thu, 15 Jun 2006 21:46:30 +0000

<http://www.lotterypost.com/news-112702.htm>

<http://www.cbsnews.com/stories/2005/04/01/national/main684584.shtml>

Powerball lottery officials suspected fraud: how could 110 players in the

March 30 drawing get five of the six numbers right? That made them all

second-prize winners, and considering the number of tickets sold in the 29

states where the game is played, there should have been only four or five.

Answer: They all chose their numbers from fortune cookies from the same

factory in Long Island City, Queens. (The unexpected payout totaled \$19

million for the second-place winners.)

Howard Israel, CEO, Secure Systems Consulting, LLC (732) 613-9464

✶ Wily crows disconnect wired Tokyo

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

Sat, 17 Jun 2006 14:10:39 PDT

"Tokyo's futuristic image as the world's most technologically advanced broadband Internet-enabled city is under attack from a vicious but decidedly low-tech foe: the crow." During the spring mating season, the crows have discovered that fiber-optic cable makes great nesting material, and have seriously disrupted Internet service. [Source: Leo Lewis, Australian IT News, 16 Jun 2006; PGN-ed; thanks to Dan Farmer for pecking out that one.]

✶ Another risk of electromagnetic interference

<Tom Philp <tphilp@bfree.on.ca>>

Sat, 17 Jun 2006 10:54:04 -0700 (PDT)

I have a Toshiba satellite P30 laptop and a Treo 650 cell phone. Recently I was working on the laptop and had occasion to take a phone call on my cell. I needed some information for the phone call, so I looked it up on my computer. To do so, I had to put my cell phone down. I placed it on the

table right next to the laptop.

Right in the middle of my Internet query, the laptop just completely shut down... no warning, just dead. When I thought about it, it seemed almost obvious that the electromagnetic radiation from the phone caused some problem and shut the system. down. I was able to reproduce this effect simply by laying the phone within a few centimetres from the computer.

While I did not lose anything, even in my testing, it does point out a problem with our computers and the ubiquity of cell phones. Surely computer manufacturers could design some kind of shielding for computers to keep them from this sort of risk.

Volvo's self braking car

<David Magda <dmagda@ee.ryerson.ca>>

Mon, 12 Jun 2006 20:13:24 -0400

I ran across this video (via Gizmodo) demonstrating Volvo's new braking system:

<http://www.youtube.com/watch?v=y9c3V0q8cgk>

It is currently in the lab, and NOT in production. Basically, if the system determines that a collision is unavoidable it automatically applies the brakes to try to prevent the collision.

Is driving safer when drivers are not involved?

RFID "Best Practices" (CDT via Monty Solomon)

✶ Risks of Ajax and Javascript

<Charlie Wertz <CharlieWertz@rochester.rr.com>>

Tue, 20 Jun 2006 09:46:09 -0400

Here is an article on the potential evils of Ajax (the use of Javascript for interactions with databases).

"Companies are quickly embracing Ajax and related techniques for Web applications. Expect more security problems like the Yamanner worm along the way. The Yamanner worm that infested Yahoo Mail last week was quickly squashed. In the 24-hour period it thrived, though, the worm provided a glimpse of what's in store for Internet users unless companies apply strict measures when building Web applications with techniques such as Ajax."

http://www.ddj.com/189500417?cid=RSSfeed_DDJ_All

I've noticed that more and more web sites just flat out won't work if I have Javascript turned off. We're not addressing sites that want to hurt us here. The technology puts us at risk when the code is merely poorly written.

✶ Ironic risk of using a 'free' mail service

<Mike Scott <usenet.10@scotts.dnsalias.com>>

Tue, 20 Jun 2006 12:26:17 +0100

I was puzzled when I saw in the mail log that some mail accepted for my wife had been flagged as spam by spamassassin, as the sender address was one of her friends. "Obfuscated reference" to a certain drug, amongst other things. I assumed the friend's machine had been hijacked, but not so. It turned out simply that yahoo had tacked on an advert for /anti/-spam software: "Tired of Vi@gr@! come-ons? Let our SpamGuard protect you". The irony is quite delicious!

Interestingly, the ad had only been inserted into the html alternative text - which we don't use anyway. A nice exercise in how to get your customers' email binned for no obvious reason.

[And that may be sufficient to cause this issue of RISKS to be blocked.

PGN]

⚡ DoE Discloses Data Theft (From Dave Farber's IP)

<Ari Ollikainen <Ari@OLTECO.com>>

June 10, 2006 1:37:31 PM EDT

Foot dragging on an incident which occurred in September 2005...

A hacker stole a file containing the names and Social Security numbers of

1,500 people working for the Department of Energy's National Nuclear

Security Administration last September. But this was not

reported to senior DoE officials until Jun 2006, and none of the victims was notified.

[Source: Energy Dept. Discloses Data Theft; Victims, Top Officials Were Not Told About 2005 Hacking, Associated Press item in *The Washington Post*, 10

Jun 2006; PGN-ed]

<http://www.washingtonpost.com/wp-dyn/content/article/2006/06/09/AR2006060901505.html>

✶ Testing stolen credit card numbers

<Walt Daniels <wdhiker@optonline.net>>

Wed, 14 Jun 2006 23:05:20 -0400

Our Verisign account on www.sample-non-profit.org is being used to test stolen credit cards. They are spoofing our IP address, so aren't even going through our web pages which contain no authorize transactions, which is what they are using to test cards. They hit us with about 20 new cards most evenings between 2am and 3am. Some succeed and some fail. The names are totally bogus, but the addresses look real. They have CVC codes and those usually match as does AVS. I assume they make use of the cards on other sites because our site has donations and memberships as well as very specialized books and maps that would be hard to sell. Sorting through all these bogus transaction, more then 50% of all our transactions, places a large load on our bookkeeper. Verisign has been very unhelpful in stopping the transactions. They claim it is the banks that are authorizing

the transactions and they are just a passthrough agency. We do not have access to the full card numbers and cannot tell which banks are involved. In some sense I am observing an ongoing crime that effects me very little. I don't know the real victims at all and cannot contact them to warn them that their card is in play.

Given enough zombies, this looks like a way of finding valid cards without having to steal them. See [Risks24-32](#) "Unsalted Credit cards" for some of the key pieces of doing this.

There are many opportunities for either the banks or Verisign to have noticed these sorts of problems, e.g. 20 transactions from a single IP address in a few minutes should be suspect. A name like "Kkkky Dhgmop" is not likely to be a real person (an actual example that was accepted).

Neither any bank nor Verisign has made any attempt to contact me to find out what I know. From the data I see I could easily be the person entering those transactions.

RFID "Best Practices"

<Monty Solomon <monty@roscom.com>>

Fri, 9 Jun 2006 20:19:58 -0400

Policy Post 12.09: CDT-Led Working Group Releases RFID "Best Practices"

A Briefing On Public Policy Issues Affecting Civil Liberties
Online from The
Center For Democracy and Technology

- (1) CDT-Led Working Group Releases RFID "Best Practices"
- (2) Best Practices Ideal for Evolving Technology
- (3) Technology-Neutral Consumer Privacy Legislation Still Needed
- ...

<http://www.cdt.org/publications/policyposts/2006/9>

Bank's redirector helps phishing

<fred bone <fred.bone@dial.pipex.com>>

Tue, 20 Jun 2006 12:05:27 +0100

I received a "phishing" email claiming to come from Barclays Bank. All the usual stuff, except that the URL it gave appeared to be plausible:
<http://www.barclays.co.uk/cgi-bin/gotosite.cgi?location=%68%74%74%70%3a%2f%2f0xc1.0xaf.0x16.0x2d%2fcache%2fbarclays.ssl%2f>

The bit after "location=" translates to
"<http://193.175.16.45/cache/barclays.ssl/>"

An experiment shows that, yes, Barclays do have a redirector which will happily redirect off-site. An absolute gift to phishers and suchlike.

[Certainly suggests a fissure of security. PGN]

Microsoft Patches crash IBM Midrange Consoles

<Al Mac <macwheel99@sigeom.net>>

Mon, 19 Jun 2006 13:20:56 -0500

Windows Patches break Operations Console of IBM midrange platform.

In the olden days of networks, a dumb terminal might have been used for IT staff to manage large computer networks. In recent years the move has been to use a PC for that function, which of course needs Windows patches. The latest round of MS patches has busted the ability of IBM Consoles to do their primary tasks.

V#R# is version of IBM operating system affected.

<http://www.itjungle.com/tfh/tfh061906-story05.html>

Re: Man Gets \$218 Trillion Phone Bill (Gold, [RISKS-24.29](#))

<"Nancy Bogart" <nancy.bogart@gmail.com>>

Tue, 20 Jun 2006 13:29:56 -0400

This reminds me of one of my first assignments in my graduate numerical analysis class: Invert a Hilbert matrix using pencil and paper and fractional arithmetic, and, invert it using a computer program. The Hilbert matrix is ill-conditioned (<http://en.wikipedia.org/wiki/Ill-conditioned>) because the fractions cannot be precisely represented in binary format, which introduces round-off error, so calculation of the inverse by computer results in greater inaccuracies as the errors are multiplied by each iteration of the algorithm. The lesson learned was, know the limits of your

computer's architecture. Five decimal places does not mean five decimal places of accuracy. [See http://en.wikipedia.org/wiki/Hilbert_matrix]

Re: Hospitals have dramatically reduced unnecessary deaths (R-24.32)

<Peter R Cook <PCook@wisty.plus.com>>

Thu, 15 Jun 2006 11:07:04 +0100

Is it just me, or have "lies, damn lies and statistics " simply become the norm in the media.

> A campaign to reduce lethal errors and unnecessary deaths in U. S.

> hospitals has saved an estimated 122,300 lives in the last 18 months. ...

With 6731 hospitals in total in the US [*], this implies that the measures, if applied to all would have saved over 265,000 lives in the last 18 months, or 177,000/year -- almost twice the upper estimate of those dying from errors and low-quality care. (I am presuming here that hospital acquired infection low quality care.)

Either someone needs a quick course in basic numeracy, that or the quality of care and error rates have soared in the US since 1999!

* http://www.hospitalmanagement.net/ihf/publication_5_1.html

[The report seemed rather overhyped to me. PGN]

Cyberwar

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

Mon, 19 Jun 2006 14:40:31 PDT

Cyberwar, Netwar and the Revolution in Military Affairs
Edited by Edward Halpin, Philippa Trevorrow, David Webb and
Steve Wright
Palgrave Macmillan, 2006

This book is based on a summer program of the International
School of
Disarmament and Research on Conflicts (ISODARCO), with a preface
by the
organizers, Gary Chapman, Diego Latella, and Carlo Schaerf, and
contributed
chapters from the lecturers. [Gary Chapman has contributed
various items to
RISKS over the years, beginning with volume 1. Disclaimer: PGN
is one of a
very diverse set of the authors.]

REVIEW: "Information Security and Employee Behaviour", McIlwraith

<Rob Slade <rMslade@shaw.ca>>

Thu, 15 Jun 2006 10:39:42 -0800

BKISEMBE.RVW 20060520

"Information Security and Employee Behaviour", Angus McIlwraith,
2006,
0-566-08647-6, U\$99.95
%A Angus McIlwraith Angus.McIlwraith@btinternet.com

%C Suite 420, 101 Cherry Street, Burlington, VT 05401-4405
USA
%D 2006
%G 0-566-08647-6
%I Gower Publishing Limited
%O U\$99.95 www.gowerpub.com info@gowerpub.com
%O [http://www.amazon.com/exec/obidos/ASIN/0566086476/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0566086476/robsladesinterne)
[http://www.amazon.co.uk/exec/obidos/ASIN/0566086476/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0566086476/robsladesinte-21)
%O [http://www.amazon.ca/exec/obidos/ASIN/0566086476/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0566086476/robsladesin03-20)
%O Audience i+ Tech 2 Writing 3 (see revfaq.htm for explanation)
%P 169 p.
%T "Information Security and Employee Behaviour"

In the introduction, McIlwraith points out that security awareness training properly consists of communication, raising of issues, and encouragement to modify behaviour. (This will come as no surprise to those who recall the definition of training as the modification of attitudes and behaviour.) He also notes that security professionals frequently concentrate solely on presentation of problems. The remainder of the introduction looks at other major security activities, and the part that awareness plays in ensuring that they actually work.

Part one looks at a "framework for understanding." Chapter one addresses employee risk, and the fact that people assess risk very poorly. Issues such as whether the risk is controlled by the self or another, problems that are diffuse or dispersed, and immediacy all reduce our perception of the scale of the hazard. Other psychological reasons for poor decision-making are also examined. (There is also some explanation as to why

security

people get fixated on their field, and often over-emphasize minor problems.)

This material definitely provides an understanding of the problem for anyone

involved in security awareness, but unfortunately does not give equivalent

solutions. The discussion of culture, in chapter two, describes a number of

diverse corporate styles, with suggestions for the type of approach most

likely to be effective in each. The fact that security

professionals are

frequently perceived as problem-creating, rather than problem-solving, is

hardly a surprise, and so neither is chapter three. However, it does

outline various reasons for this perception, which may give us insight into

changes we could make. (I'm finishing off the security dictionary manuscript at the moment [www.syngress.com/catalog/?pid=4150], and

McIlwraith's comments on the jargon we use in security are definitely

cringe-making.)

Part two moves into solutions. Chapter four outlines practical strategies

and techniques. The author lists five major points: manage by facts and

reality (rather than vague desires), have specific objectives (instead of

just "we need training"), plan carefully, implement meticulously, and get

real feedback on the results. Additional mechanisms for training success

are discussed. Realistic assessment of the program (and the danger of

simple metrics) is reviewed in chapter five. (I might take slight exception

to McIlwraith's recommendation on rating scales: any use of odd-numbered

scales tends to push responses into the middle.) Design of the delivery

media for awareness materials is as important as the message, and chapter six provides useful advice for those of us who are stylistically challenged--which includes pretty much the entire technically-oriented clan.

McIlwraith's message is important. His writing is interesting and clear.

His suggestions are useful. His book is recommended for anyone with either

a specific obligation for awareness training, or overall responsibility for security management.

copyright Robert M. Slade, 2006 BKISEMBE.RVW 20060520

rslade@vcn.bc.ca slade@victoria.tc.ca

rslade@computercrime.org

<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

Search RISKS using [swish-e](#)

Volume 24: Issue 34

Wednesday 19 July 2006

Contents

- [Computer closes Berlin tunnel again](#)
[Debora Weber-Wulff](#)
- [B747 freighter crash](#)
[Peter B. Ladkin](#)
- [Y2038 bug strikes early](#)
[Conrad Heiney](#)
- [One fewer risk](#)
[R.A. Whitfield](#)
- [Yet another example of accidental disclosure of redacted info](#)
[Aaron Emigh](#)
- [More university data exposures](#)
[PGN](#)
- [Deceiving a computer is now a crime](#)
[Vassilis Prevelakis](#)
- [Risks of increasingly complex hardware/software in rescue gear](#)
[Fernando Pereira](#)
- [Unexpected electromagnetic interference](#)
[Ken Winters](#)

- [Companies still unclear on authentic e-mail transmission](#)
[Steve Summit](#)
 - [Re: Sunken Ferry Crew didn't know how to use ECS display software](#)
[Joseph A. Dellinger](#)
 - [Re: Microsoft Patches crash IBM Midrange Consoles](#)
[Henry Baker Al Mac](#)
 - [REVIEW: "How to Break Web Software", Mike Andrews/James A. Whittaker](#)
[Rob Slade](#)
 - [REVIEW \(sorta\): "Dictionary of Information Security", Robert Slade](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Computer closes Berlin tunnel again

<"Debora Weber-Wulff" <D.Weber-Wulff@fhtw-berlin.de>>

Tue, 4 Jul 2006 20:27:31 +0200 (CEST)

The Berlin newspaper reports on July 4, 2006

[<http://archiv.tagesspiegel.de/archiv/04.07.2006/2638585.asp>]

on another computer-caused tunnel-closing (a previous episode is in

[RISKS-24.09: http://catless.ncl.ac.uk/Risks/24.09.html#subj1.1](http://catless.ncl.ac.uk/Risks/24.09.html#subj1.1)).

Seems about 1am the central computer lost contact with the traffic system in the tunnel. A technician was aroused, but he pointed out that the city had not signed a support agreement in order to save money, so he was not on call at nights.

An accident occurred in the tunnel with a car flipping over. The sensors reported the problem, but because the central computer could not communicate with the system in the tunnel, it could not be closed. The car caught fire,

and the smoke alarmed more sensors that were programmed to automatically close the tunnel (with the accident victim inside).

Since one of the gates was not closing (it had been demolished but not repaired), the out-of-control system went into fail-safe mode and turned all of the traffic lights red.

Even in the middle of the night, Berlin never sleeps (and especially so during a World Cup in Soccer), so the traffic piled up with no one being able to go anywhere near the tunnel. Police were called to direct traffic and get the accident car and victim out (who was unhurt, if ruffled) by about 5.30 am, shortly before rush hour begins (7.30 is a normal working day start in the eastern parts of Berlin).

The computer refused to budge from the fail-safe mode. They called the technician again (who was now awake, anyway). He agreed to come in, but could not get the system to restart, either, until he cut through the cabling to get a cold-start on the traffic lights on the major streets. It took another few hours to get everything working again.

MTBPF (mean time between published failure): 7 months.

Prof. Dr. Debora Weber-Wulff, FHTW Berlin, FB 4, Treskowallee 8, 10313 Berlin
GERMANY +49-30-5019-2320 <http://www.f4.fhtw-berlin.de/people/weberwu/>

B747 freighter crash

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>

Tue, 04 Jul 2006 13:17:36 +0200

The Canadian TSB have issued the report on the 14 October 2004 crash of a Boeing B747 freighter on takeoff at Halifax airport, Nova Scotia.

According to a Flight International report by David Kaminski-Morrow (4-10 July 2006, p4), the TSB "says that the crew's misunderstanding of a laptop computer tool for calculating take-off performance led to the accidents. It concludes that the crew unwittingly transferred and used weight data from the aircraft's previous flight while calculating performance criteria for the next take-off. The obsolete data misled the crew to derive incorrect thrust settings and critical speeds for take-off."

The aircraft failed to lift off after rotation and overran the end of the runway by 250 meters, briefly lifting off but then striking an earth berm, severing the tail section and bringing the aircraft to earth again. All seven crew were killed.

This is the second laptop-involved accident to be reported (but the first to have occurred). The Southwest Airlines accident in 2005, also a runway overrun but on landing, was discussed in [Risks-24.15](#) (Thompson), 24.16 (Ladkin, dwikstrom), 24.17 (Norman) and subsequently (24.18, 24.19).

Peter B. Ladkin, Causalis Limited and University of Bielefeld
www.causalis.com www.rvs.uni-bielefeld.de

⚡ Y2038 bug strikes early

<Conrad Heiney <conrad@fringehead.org>>

Thu, 29 Jun 2006 13:38:25 -0700

Starting on May 12, 2006, many installations of the AOLServer web server failed. Not all versions or all configurations failed, but the ones that did became unusable. On start, the server would eat virtual memory and then terminate with a memory allocation error. Discussion on the mailing list revealed the starting date of the problem, indicating that some part of the software had a clock issue. On careful inspection it was discovered that database threads were a common factor. It was then noted by a perceptive person that the servers all failed on or before exactly one billion seconds before the end of the Unix epoch in 2038. Many installations had very long database timeouts, which caused the software to look ahead and see the End of Time. Adjusting the timeouts stopped the crashes.

The risk of the known clock bug striking 32 years early indicates there may be other "pre-problems" lurking in software that will show up long before the date we have comfortably set as the deadline.

The thread discussing the problem and its resolution is here:
<http://www.mail-archive.com/aolserver@listserv.aol.com/msg09812.html>

✂ One fewer risk

<"R. A. Whitfield" <inquiry@quality-control.us>>

Sun, 25 Jun 2006 05:47:48 -0400

Abatement of a risk posed by computing is only occasionally noted in RISKS.

So it is a pleasure to announce a risk that has been eliminated altogether.

Robert Siegal, the co-host of National Public Radio's "All Things Considered" program, interviewed Stuart Levey, the Under Secretary for Terrorism and Financial Intelligence at the Department of the Treasury, on the June 23, 2006 program. The two discussed the recent revelation of a surveillance program of banking transactions conducted by the Treasury Department in association with the Society for Worldwide Interbank Financial Telecommunication (SWIFT) in Brussels. An audio recording of the interview can be found at <http://www.npr.org/templates/story/story.php?storyId=5507148>

Mr. Siegal expressed concerned that the surveillance of a tremendous amount of financial data might be viewed as a "fishing expedition."

He was reassured by Mr. Levey as follows: "Well, actually I think there's a little bit of misconception there... We have a set of data that is provided to us by SWIFT. But in fact we cannot access it just to do whatever we want - to browse through it, for example, or to do broad searches. Instead, we can only access it if our analyst first explains exactly who or

what wants

to do a search on and then articulates how that person or entity is connected to an ongoing terrorism investigation."

Q. (by Mr. Siegal) "To whom is that person explaining and articulating those conditions?"

A. (by Mr. Levey) "Well, the way it works is the analyst has to type that into the database and cannot access the database until that has been accomplished. And there are two sets of auditors that are monitoring what is going on. One, in a very, I think, creative and unusual arrangement that we set up with the company, with SWIFT... SWIFT itself is on site and has real time access to all the searches that are being done and at any time their representatives can stop the search and say, 'Wait a minute. I have a question about that. I'm not sure why that's connected to terrorism or the connection hasn't been articulated sufficiently.' And then, after the fact, it can be audited both by SWIFT and by outside auditors that we've engaged to do just that."

The risk eliminated by Mr. Levey's explanation is, of course, the risk that anyone will believe an official statement from the U.S. Treasury Department about the Department's surveillance activities.

R.A. Whitfield inquiry@quality-control.us www.quality-control.us

[Reminder: RISKS has **always** had a policy of eagerly welcoming items relating to the avoidance of risks through good practices, or

even

accidentally! Unfortunately, they are rarely submitted (and this one is

of course not an exception). By the way, my regrets for the long hiatus

between the previous issue and this one. This year's seasonal slowdown

has been slower than usual. PGN]

Yet another example of accidental disclosure of redacted info

<"Aaron Emigh" <aaron-risks@radixlabs.com>>

Thu, 22 Jun 2006 14:56:39 -0700

This article reports on yet another case in which an electronic document

with redactions actually contains all of the redacted data:

<http://www.nytimes.com/2006/06/22/washington/22cnd-leak.htm>

After many such incidents, it seems a reasonable conclusion that complex

document formats that permit overlays, such as Word and PDF, are too prone

to misuse when information is intended to be redacted. In a closely related

issue, buffers in many document formats can inadvertently contain sensitive

information that the author has intended to delete.

It seems clear that only simple electronic document formats - preferably

just imaging formats such as TIF/GIF/PNG - are suitable for use in cases

where sensitive information is intended to be excluded from an edited

document. Even then, the inclusion of a step that removes the possibility

of contamination beyond the visible content - such as faxing to

a fax
machine and scanning the fax in - may be advisable.

Aaron Emigh, Radix Labs 1-415-297-1305

⚡ More university data exposures

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

Wed, 21 Jun 2006 12:06:29 PDT

Two universities last week reported incidents in which outsiders may have gained access to personal information, including Social Security numbers, of a total of up to nearly a quarter-million students. [On 13 Jun,] Western Illinois University announced that a hacker may have copied Social Security or credit-card numbers of between 200,000 and 240,000 current or former students. The credit cards had been used to purchase textbooks online or for stays in a university hotel. [Source: Vincent Kiernan, Incidents at 2 Universities Put More Than 200,000 Students at Risk of Data Theft, The Chronicle of Higher Education, 19 Jun 2006]

⚡ Deceiving a computer is now a crime

<Vassilis PREVELAKIS <vp@drexel.edu>>

Sun, 16 Jul 2006 05:00:35 -0400 (EDT)

Earlier this year the UK Attorney General introduced an

amendment to the
Fraud Bill to make "deceiving a computer" a criminal offense.
While the
intention (preventing people from hacking chip-and-PIN devices)
is
worthwhile, the attempt to attribute human characteristics to
machines is
bound to cause problems. I was going to write something on the
subject when
I discovered that this has already been discussed in this forum
18 years
ago!

Risks Volume 7: Issue 69, Thursday 3 November 1988

dan@WILMA.BBN.COM wrote:

> Tue, 01 Nov 88 16:39:47 -0500

>

> Re the Confederation of British Industry's proposal to change
the law on

> defrauding to include deception of computers as well as people:

>

> To state the obvious, computer programs are so limited in
their ability to

> understand what someone might be trying to do, and what
information is

> necessary for that purpose, that it's often necessary to
"deceive" them

> just to get them to do the right thing. It's much like the
problem of

> figuring out what to put on a complex form, like tax forms:
every

> individual situation is different, and the form either
provides no way at

> all to say what your situation is, or provides several equally
plausible

> ways to express it. But at least forms have margins, and you
can attach

> additional pieces of paper to them. Computer-based "forms"
have neither.

> Here's an example: in the process of trying to provide some
service, a

> computer asks for my telephone number. I don't believe it has

any right to
> that number for this purpose, so I refuse to answer. But it
won't go on to
> the next query until I answer that one. I find someone in
charge: "I don't
> want to give my phone number out. Is that OK?" "Sure. Just
give it a fake
> number and go on." The computer is now "deceived". It's
ridiculous to
> think that both I and the computer's owner could now be
charged with
> fraud!
>
> Taken literally, such a law would also preclude thorough
testing of
> computer software. In testing, you're almost always
"deceiving" the
> computer in order to see whether it will handle some case
correctly,
> particularly if you're checking error handling. Are testers
going to have
> to insert special routines that print out "It's OK, I know
this is a test"
> before giving any answers, to avoid prosecution?
>
> There are also serious theoretical problems with the notion of
"deceiving"
> a computer. In theory, deception occurs when an individual is
deliberately
> led to believe X when not-X is true. But what does "belief"
mean when
> applied to a computer system? If I have a file on a computer
system that
> says I'm 3 years old, does that mean the computer "believes"
I'm three
> years old? Of course not, you say. What if it's in a database?
Is it
> deception then?
>
> I think it's all the fault of some AI people who would like us
to think
> that all it takes to be able to say that a computer system
believes a fact

> is that it's in a Lisp-based inference system that includes a
> "believes"
> predicate!
>
> Dan Franklin

They never give up, do they?

✦ Risks of increasingly complex hardware/software in rescue gear

<Fernando Pereira <pereira@cis.upenn.edu>>

Fri, 30 Jun 2006 16:31:19 -0400

Avalanche beacons have been undergoing rapid development as low-power DSP technology improves and pursuits like backcountry skiing grow in popularity. For those readers who don't know about these beacons, here's a description <http://www.telemarkski.com/html/how_beacon_select.html>. A beacon is carried strapped to the user's upper body. In its default on state, it transmits a regular signal at 457khz. If the user is buried by an avalanche, other members of the group turn on their beacons to receive mode. In receive mode, a beacon can be used to follow flux lines from the transmitting beacon to locate the buried beacon and the user to which it is strapped. Ease of operation by rescuers is critical, since chances of survival for the buried victim decrease rapidly after 20 minutes under the snow. Therefore, modern beacons have gained increasingly sophisticated DSP features that facilitate tracking a transmitting beacon, and also distinguishing among multiple signals in a multiple burial

situation. Not so long ago, a newly released and highly touted beacon model had to receive a firmware update because of concerns with its multiple burial detection software. Now, one of the leading vendors has introduced a beacon that claims to signal to like beacons whether the buried victim is still alive, allowing rescuers to move on to dig out those victims that are still alive

<

concern among experienced backcountry skiers. What if rescuers rely on this feature, but a transmitting beacon fails to detect its user's vital signs? Conversely, what if a beacon hallucinates vital signs that are not there? What are the responsibilities of rescuers relative to possible beacon-generated misinformation? What are their responsibilities dealing with a multiple burial where some of the beacons do not have the feature? Does the additional (mis?) information add to the cognitive and emotional overload that is well known to affect decision-making among rescuers? We have limited capacities, should those part of those limited capacities be devoted to adjudicating these difficult issues in a life-or-death situation?

⚡ Unexpected electromagnetic interference

<Ken Winters <k27winters1@comcast.net>>

Wed, 28 Jun 2006 20:45:52 -0400

Shortly after reading the item about the laptop seizing up when the cell

phone was put next to it, I used my kitchen scale (digital, but hardly a complex piece of electronic equipment) while I was using my cordless phone. The scale wouldn't keep a stable "zero" setting. With some trial and error, I found that accessing the stored information (previous calls and directory) would cause the scale reading to briefly change by as much as 34 grams. In 5 to 10 seconds it returned to normal.

Hardly serious, at least in this case, but it reminds us: "Expect the Unexpected"!

✶ Companies still unclear on authentic e-mail transmission

<Steve Summit <scs@eskimo.com>>

Sun, 09 Jul 2006 20:44:06 -0400

I received e-mail from PayPal the other day -- **real** e-mail, not one of the 15-20 PayPal-branded phishing scams I get each day. I was pleasantly surprised that it made it past my spam filter, and I was curious to see what sorts of things PayPal is doing these days to assure recipients that their missives **are** genuine. Answer: not much, and in fact the first Received line -- which as we know is about all you can trust in an ordinary e-mail -- indicated that it came from "protege.postdirect.com", i.e., some third party. Sigh.

✈ Re: Sunken Ferry Crew didn't know how to use ECS display software

<"Joseph A. Dellinger" <geojoe@freeusp.org>>

Thu, 22 Jun 2006 23:00:44 -0500

(Manning, [RISKS-24.33](#))

At the George Observatory near Houston Texas we also need to "dim down the display" so we can work in near darkness while imaging 20th-magnitude asteroids. We used to have a monitor with an analog wheel that could be used to control the display brightness. Alas, it seems that all the modern monitors adjust their brightness with button controls. Changing the brightness up and down is a pain to do, and the display that comes up while changing the brightness is itself uncontrollably bright. You can use Windows to change the "theme" to something red and dim, but then some important control menus in programs we need come up black on black, and so are unusable.

Our solution was a red piece of plastic the size of the monitor held on with Velcro. Pops on (for dim) and off (for bright), and never causes any software incompatibility issues. :-)

The risk? Insisting on a software solution for a software problem. Although the folks on the ferry did come up with a hardware solution (turning the monitor off) it wasn't a very good one!

⚡ Re: Microsoft Patches crash IBM Midrange Consoles (Macintyre, R-24.33)

<Henry Baker <hbaker1@pipeline.com>>

Tue, 20 Jun 2006 13:36:28 -0700

This is not a new problem for IBM. My first job in high school was looking after a large (at that time!) 7040 system which utilized an (IBM, of course!) selectric typewriter as the system console.

Guess which I/O device on the 7040 caused the most down-time ?

(Hint: not the tape drives, the printer, the front-end 1401 or the card reader/punch...)

⚡ IBM Patch Troubles

<Al Mac <macwheel99@sige.com.net>>

Thu, 22 Jun 2006 11:05:44 -0500

While there are a FEW people in IBM Customer Land who apply patches without reading the instructions, or researching the gotchas, I imagine there are a LOT of people in Microsoft Customer Land in that boat. The difference is the rate of patches, the likelihood of problems, and number of occupants of Customer Land who consider what is being patched to be mission critical.

<http://www.itjungle.com/tfh/tfh061906-story02.html>

REVIEW: "How to Break Web Software", Mike Andrews/James A. Whittaker

<"Rob, grandpa of Ryan, Trevor, Devon & Hannah" <rMslade@shaw.ca>>
Mon, 26 Jun 2006 11:46:59 -0800

BKHTBWSW.RVW 20060520

"How to Break Web Software", Mike Andrews/James A. Whittaker,
2006,
0-321-36944-0, U\$34.99/C\$46.99
%A Mike Andrews Mike.Andrews@foundstone.com
%A James A. Whittaker jw@cs.fit.edu
%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8
%D 2006
%G 0-321-36944-0
%I Addison-Wesley Publishing Co.
%O U\$34.99/C\$46.99 416-447-5101 800-822-6339 bkexpress@aw.com
%O [http://www.amazon.com/exec/obidos/ASIN/0321369440/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0321369440/robsladesinterne)
[http://www.amazon.co.uk/exec/obidos/ASIN/0321369440/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0321369440/robsladesinte-21)
%O [http://www.amazon.ca/exec/obidos/ASIN/0321369440/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0321369440/robsladesin03-20)
%O Audience i+ Tech 3 Writing 2 (see revfaq.htm for
explanation)
%P 219 p. + CD-ROM
%T "How to Break Web Software"

The preface stresses that this book is neither about how to
attack a
Web site, nor how to develop one, but, rather, how to test.

Chapter one points out that the Web is a different environment,
in
terms of software security, because we have desktop machines, not
centrally administered, talking to everyone (with much of the

traffic

being commercial in nature). The authors even point out that issues of error-handling, performance, and ease-of-use all contribute to increased levels of vulnerability. Various attacks designed to obtain information about Web applications, structure, and functions are described in chapter two. For client-side scripting, chapter three notes, any validation done on the client should be untrusted and re-validated on the host, since it may be altered on the client, or data manually entered as if it came from the client. Chapter four explains the danger of using client-side data (cookies or code) for state information. Chapter five examines user supplied data, and delves into cross-site scripting (XSS, the explanation of which is not well done), SQL (Standard Query Language) injection, and directory traversal. Language-based attacks, in chapter six, involve buffer overflows (which are not explained terribly well), canonicalization (HTML and Unicode encoding and parsing), and null string attacks. The server, with utilities and the underlying operating system, can be reached via stored procedures (excessive functionality), fingerprinted for other attempts, or subject to denial of service (in limited ways) as chapter seven notes. "Authentication," in chapter eight, is really more about encryption: the various false forms (encryption via obscurity?), brute force attacks against verification systems, and forcing a system to use weak encryption. Privacy, and related Web technologies (of which cookies are only one), is reviewed in chapter nine. Chapter ten looks at Web services, and the vulnerabilities

associated with some of these systems.

The CD-ROM included with the book contains a number of interesting and useful tools for trying out the various attacks and tests mentioned in the text.

This book is a valuable addition to the software security literature.

The attacks listed in the work are known, but often by name only. This text collects and explains a wide variety of Web application attacks and weaknesses, providing developers with a better understanding of how their programs may be assailed. Some of the items mentioned are defined or explained weakly, but these are usually items that do have good coverage in other security works.

copyright Robert M. Slade, 2006 BKHTBWSW.RVW 20060520
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>

REVIEW (sorta): "Dictionary of Information Security", Robert Slade

<"Rob, grandpa of Ryan, Trevor, Devon & Hannah" <rMslade@shaw.ca>>
Fri, 07 Jul 2006 17:31:47 -0800

BKDCINSC.RVW 20060528

"Dictionary of Information Security", Robert Slade, 2006,
1-59749-115-2, U\$29.95/C\$38.95

%A Robert Slade rslade@vcn.bc.ca

%C 800 Hingham Street, Rockland, MA 02370

%D 2006

%G 1-59749-115-2

%I Syngress

%O U\$29.95/C\$38.95 781-681-5151 fax: 781-681-3585 amy@syngress.com
%O <http://www.amazon.com/exec/obidos/ASIN/1597491152/robsladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/1597491152/robsladesinte-21>
%O <http://www.amazon.ca/exec/obidos/ASIN/1597491152/robsladesin03-20>
%O <http://www.syngress.com/catalog/?pid=4150>
%O Audience n+ Tech 3 Writing 3 (well, I would, wouldn't I?)
%P 256 p.
%T "Dictionary of Information Security"

Their our lots of wurdz in this book. Sum of the werds are big. They're are no pitchers in this book. If ewe like big wirds and no pitchers you will like this book. [Nut meny mispelinz in the book, though. PGN]

The courier driver showed up at noon, today, with the box of author copies. So I can, with assurance (p. 13) state that the volume now actually exists in hardcopy. After four years of maintaining it mostly as a resource for those studying for the CISSP exam, it's now going to be available in bookstores for everyone.

It's been interesting, working with Syngress. Having worked with more traditional publishers, I was rather expecting the usual 2-3 months of contract negotiations, 2-3 months to get out the final manuscript (the book had, after all, already been basically finished: I'd been using it on the Website for some time), and the usual 4-6 months in copy editing and galley proofing. The contract negotiations took about a month and a half. I got

the final contract May 18th. They wanted the manuscript on the 26th. I got the galley proofs on June 1st, and had them back to Syngress on June 4th.

(Then there seems to have been some kind of hiccup with the printer: it's been "due" every day now for about three weeks.)

So now, I suppose, I'd better get a move on. I've already replaced the glossary page (<http://victoria.tc.ca/techrev/secgloss.htm>) with an errata page, and I've got about 60 entries that need to be added or corrected. So I hope you'll all actually buy the book, and Syngress will be moved to putting out a new edition fairly soon. (And regularly, after that.)

copyright Robert M. Slade, 2006 BKDCINSC.RVW 20060528
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<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

Search RISKS using [swish-e](#)

Volume 24: Issue 35

Thursday 20 July 2006

Contents

- [Air traffic control snafu around LAX](#)
[PGN](#)
- [20 inspectors suspended over refusing GPS cellphones](#)
[Monty Solomon](#)
- [PlusNet obliterates customers' e-mail](#)
[Mary Ellen Foster](#)
- [IEEE e-mail alias service with Comcast](#)
[Pete Klammer](#)
- [MSN Messenger blocking URLs on server side](#)
[Cody B](#)
- [Dirty Data contaminates Business Decisionmaking](#)
[Al Macintyre](#)
- [Corporate Risks](#)
[Al Macintyre](#)
- [Banks not yet aware enough of phone-phishing](#)
[John Pettitt](#)
- [The Risks of retro computing?](#)
[Edward G. Nilges](#)

- [Risks of relying on the Web in wartime](#)
[Tim Chmielewski](#)
 - [Re: Yet another example of accidental disclosure of redacted info](#)
[Amos Shapir](#)
 - [Re: Subject: Deceiving a computer is now a crime](#)
[David H Smith](#)
 - [REVIEW: "Insider Threat", Eric Cole/Sandra Ring](#)
[Rob Slade](#)
 - [REVIEW: "Practical VoIP Security", Thomas Porter et al.](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈ Air traffic control snafu around LAX

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

Thu, 20 Jul 2006 09:35:11 -0700 (PDT)

A power blackout shut down the Los Angeles Air Route Traffic Control Center in Palmdale CA for three hours on the evening of 18 July 2006, following a power outage and the failure of the backup power system. The original power outage was caused by a pickup truck hitting a utility pole. This automatically caused a cutover to the backup power system, but the switching system failed an hour later. The Palmdale ATC was without phones (!), computers, and radar for two hours, and another hour was required to get things running again. As a result, 348 flights around the U.S. were canceled, delayed, or diverted, 221 of them at LAX. One flight from Canada to LAX was diverted to San Jose. The problem even delayed a test launch of a Minuteman III missile from Vandenberg Air Force Base, which would have

required controlled access to the airspace. [Source: Daisy Nguyen, Associated Press, seen in the *Palo Alto Daily News*, 20 July 2006; PGN-ed]

✦ 20 inspectors suspended over refusing GPS cellphones

<Monty Solomon <monty@roscom.com>>
Sun, 16 Jul 2006 23:29:34 -0400

The Massachusetts public safety commissioner yesterday suspended 20 state building and engineering inspectors for refusing to accept cellphones equipped with global positioning systems. Only two inspectors accepted the phones; another two were out on vacation when Commissioner Thomas Gatzunis tried to distribute the phones, which supervisors want to use to keep track of the inspectors during the work day. ... [Source: Andrea Estes, 20 inspectors suspended over GPS: Public safety chief metes out discipline, *The Boston Globe*, 11 Jul 2006]

http://www.boston.com/news/local/articles/2006/07/11/20_inspectors_suspended_over_gps/

✦ PlusNet obliterates customers' e-mail

<"Mary Ellen Foster" <foster@in.tum.de>>
Thu, 20 Jul 2006 10:43:35 +0100

[Source: Chris Williams, PlusNet obliterates customer e-mails; Punters cut-off by bungling storage update, *The Register*, 11 Jul 2006; PGN-ed]

http://www.theregister.co.uk/2006/07/11/plusnet_email_fiasco/

In the process of upgrading its storage management, PlusNet deleted more than 700GB of its customers' e-mail and disabled the ability of about half its 140,000 users to send and receive new e-mail. "At the time of making this change the engineer had two management console sessions open one to the backup storage system and one to live storage. These both have the same interface, and until [then] it was impossible to open more than one connection to any part of the storage system at once." Patches were installed, but the engineer assumed he was working with the backup rather than the live server. Thus, "the command to reconfigure the disk pack and remove all data therein was made to the wrong server."

IEEE e-mail alias service with Comcast

<"Pete Klammer" <NETRONICS-PE@comcast.net>>

Thu, 13 Jul 2006 17:07:29 -0600

As necessary as it is, blacklisting purportedly for SPAM control has terrible potential for abuse and mischief, especially when Internet service providers outsource the function to third parties, such as BrightMail, and entrust them with screening decisions. In my own recent

experience, known
good legitimate e-mail messages from a critical vendor (OrCAD
software) were
deleted without a trace, without recourse, without explanation,
and neither
I nor my ISP nor my address forwarder could do a damn thing
about it -- we
couldn't even get logs evidence of the deletion, nor rules
documenting
whether or not the deletion should take place (but we could
prove it by
sending the same messages to a different address). Worse, I
have seen
skewing of issue-oriented (political, etc.) e-mail being
filtered or not --
should this be in the hands of unaccountable third parties?

Dear IEEE Alias User,

... The IEEE became aware that "comcast.net" was blacklisting
IEEE's
e-mail servers. As a result "ieee.org" e-mail forwarded to
"comcast.net"
e-mail accounts was being rejected. ...

Peter F. Klammer, P.E., NETRONICS Professional Engineering, Inc.
3200 Routt Street, Wheat Ridge, Colorado 80033-5452 (303)274-
6182

[If anyone sent e-mail to me at pklammer@ieee.org, it should be
good again.]

⚡ MSN Messenger blocking URLs on server side

<"Cody B." <cody@zone38.net>>

Tue, 4 Jul 2006 12:53:06 -0400

Blogger Arve Bersvendsen, back in February of this year, posted
a summary of
a Swedish magazine article mentioning that the MSN Messenger
service (or

Live Messenger, as it's known now) has been automatically blocking the transmission of certain messages based on very primitive keyword matching
<<http://virtuelvis.com/archives/2006/02/microsoft-censoring-msn-messenger>>.

The post went largely unnoticed for much of the year, but recently it surfaced on Digg.com, where it suddenly garnered a lot more attention.

<http://digg.com/software/Microsoft_censors_MSN_Messenger>

The concept underlying MSN's block was perfectly reasonable-- they were simply trying to prevent the spread of certain worms via malicious web links.

The execution, on the other hand, was severely lacking. There's absolutely no notification to the receiver that anything was blocked, and only an extremely delayed notification to the sender.

The worst part of the execution, however, is the actual choice of strings that MSN deemed worthy of blocking. Though no master list has been made public, various users have discovered that "download.php", "gallery.php", "profile.php?", and even ".pif" and ".scr" contained anywhere in a message will prevent that entire message from going through. Apologists will rightly claim that every one of these strings has been used in the URLs of malicious worms at some point-- but there's far more potential for false positives, as a cursory Google search for "download.php" will quickly reveal, and besides, the worm writers can easily stay ahead of the block by just changing a few filenames before their next release.

The Risks here should be obvious to anyone who wishes to send a link to Dave Winer's blog at <<http://www.scripting.com/>>, the Scranton Times-Tribune at <<http://www.scrantontimes.com/>>, or any one of numerous other perfectly legitimate URLs that happen to contain one of the blocked strings.

Cody "codeman38" Boisclair cody@zone38.net <http://www.zone38.net/>

Dirty Data contaminates Business Decisionmaking

<Al Macintyre <macwheel99@sigeom.net>>
Sun, 09 Jul 2006 23:08:39 -0500

Companies can be plagued with bad dirty data. Companies make business decisions based on their data. The soundness of those decisions is negatively affected by the degree to which there is bad data.

The degree to which various CASE tools, spread sheets, queries, etc. have helped just anyone get at data, has also had the effect of lowering quality control on data going into reports, because while many people are skilled at data processing, and testing veracity of data, many are not.
<http://www.itjungle.com/tfh/tfh071006-story08.html>

Corporate Risks

<Al Macintyre <macwheel99@sige.com.net>>

Tue, 18 Jul 2006 19:33:53 -0500

What are the odds?

1 in 6 of laptop or PDA stolen

4 in 5 data files stored unencrypted

2 in 3 data files transferred unencrypted

1 in 2 limits users ability to install whatever they please,
irrespective

of risks

1 in 5 suffered data or network sabotage

1 in 4 not know if computers have been illegally accessed

2 in 5 not keep log of computer security incidents

9 in 10 suffered a computer security incident during the past
year

ALL enterprises have some software installed on desk tops that
computer

staff not know are there, and would not approve of if they did
know

Other common problems

* Systems for security, that are so complicated that no one uses
them, are

as bad as having no security at all,

* Computer systems functionality depends on various
configuration files ...

who has access to them?

* Security needs to be documented, otherwise investigators will
assume you

did not do it

* Employees bring unsecure home systems to the office, plug them
into

corporate systems and guess what? now the corporate systems are
unsecure. Example, some employee at a financial institution
had a lap top

from home with the wireless port wide open, plugs it into the
system at

work, which is now wide open over the wireless port

* Each new technology has new security weaknesses unknown to
people

installing them

* Executives consider corporate security rules do not apply to

them, they

are free to break any of them

* People think the laptop breach laws do not apply to other portable

devices that can carry corporate data ... they are wrong

* Data is backed up, but can it also be restored in a crisis ... there

should be periodic checks that backups are getting everything they ought to

What keeps IT up at night?

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

[article/06/07/17/79603_29FEnightsweats_1.html](http://www.infoworld.com/article/06/07/17/79603_29FEnightsweats_1.html)

⚡ Banks not yet aware enough of phone-phishing

<John Pettitt <jpp@cloudview.com>>

Wed, 19 Jul 2006 17:47:23 -0700

I got a call this week from a Florida number. When I answered a recorded

voice said that the fraud early warning dept of Citibank had a detected

activity on my card and would I call them back at 888-...-....

RISKS readers will no doubt see the problem here - I could be calling

anybody. Since the first thing the Citibank system asks is that you touch

tone or speak your card number customers are already expecting to give this

information. It would be trivial to also then ask for the CVV number and

exp date. Combine this with a name and address obtainable from numerous

databases to complete the data needed for fraud. With PC based VOIP systems

constructing such a scam that would call hundreds of people,

trolling for
numbers, would be close to trivial and very hard to track. I
suspect it
would actually work better than having a real human ask for the
info in that
we are all conditioned to provide whatever the auto attendant
says it needs
...

The answer is simple customers should call the number on the
back of the
card never a number given on the phone and banks should not ask
customer to
call unknown numbers.

(P.S. as it happens this call was real but a false positive, the
Citibank
system has a lot of those, but that's another risk entirely)

🔥 The Risks of retro computing?

<spinoza1111@yahoo.com>
2 Jul 2006 03:47:20 -0700

Retro computing, also known as "computation for old guys" is all
rather
charming, and creates a valuable historical record.

As an old guy who started on the IBM 1401, I suppose I should
support the
(re)building of a working 1401 at the Computer History Museum in
Mountain
View. But I have serious reservations.

The hardware system is being rebuilt down to the bare metal
using original
technology including devices of some toxicity. This adds a
somewhat useless
object to the world's stock of useless objects in view of the

fact that the IBM 1401 can be completely simulated on a modern computer without additional toxicity: without making a new artifact of questionable usability.

It will when complete demonstrate what old computing was like, which was noisy and rather satisfying if you were a young guy which I was.

However, this presents as an "important document" just one of many computers, a computer which even in 1959 had significant limitations.

The 1401 was slow even in 1959 with an 11.5 ms cycle time. It used a strange technique for addition and subtraction, called CADT (cannot add and does not try) in which transistors essentially acted as decimal addition tables. Modular programming was discouraged because there was no indirect addressing.

The 1401 was aggressively marketed by IBM worldwide in a rather dishonest campaign in which fearful, uncertain and doubtful managers were told it was nothing more than a glorified printer, an accounting machine, and not really a computer. Unfortunately it was and had marvelously arcane secrets. But, these secrets also constituted a waste of time.

What's needed in place of weekend projects for retired engineers would be a truly global encyclopedia in the form of software simulators (perhaps in the form of a computer game) for all or most early world computers.

I don't think that recreating the actual hardware of the 1401 will damage silicon valley's water table any more than it has been damaged;

yet I cannot
escape a sense of recursive inelegance in the idea of having to
rebuild a
system. Scaling up into the future, will more and more Old Guys
be involved
in recreating more and more outdated systems until we're all so
busy doing
retro computing we have no time for lunch?

When I visited the Computer Museum, I sensed somehow its
psychology to be
hardware oriented, oriented toward a work ethic in which
reification, making
a concept into a thing, reigned supreme. Lost in the reified
history is of
course the programmers who had to write a divide routine because
IBM was too
greedy to appropriately bundle the "extra cost hardware" into the
system. Lost in the reified history is the code that simulated
divide
incorrectly, and lost too is the Fortran compiler in which I
discovered a
handcoded multiply divide routine, inserted as a machine-
language patch, by
an IBM customer engineer who thought the machine had no multiply/
divide
hardware (it did) but didn't realize that there was no memory
for the patch
at all on a minimal Fortran machine.

Lost in the reified history is the story of Labor. Resources
currently
wasted in building working models of old devices could be used
to create
oral histories of early computing. Of course, such an history
would be
necessarily a critical history offensive to the sensitivities of
the
Computer Museum's corporate sponsors.bouffant

Such an history would include not the professional models who
pose so
elegantly in front of advertising snapshots of the 1401 in

business suits
and bouffant hairdos but also operators in tears and exhausted
programmers
(whose IBM training course was silent on Modify Address).

Cf. David Noble, Forces of Production. History is herstory and
history, not
itsstory, the story of devices.

What's being reassembled is a device driven too much by exchange
value and
not enough by use value. It deserves to be simulated but,
perhaps, not
rebuilt.

⚡ Risks of relying on the Web in wartime

<"Tim Chmielewski" <tim@humanedge.biz>>

Thu, 20 Jul 2006 13:03:17 +1000

Another Australian in Beirut says the Australian consulate
refused to
register his presence in Lebanon, instead referring him to a
website.

Austin Mackell has been living in Lebanon since February and
says that with
electricity out in much of Beirut it is almost impossible to
register his
presence online. (The Australian Government closed the
consulate as soon as
the bombing started.)

[http://www.theage.com.au/news/world/downer-defends-
evacuation/2006/07/20/1153166495858.html](http://www.theage.com.au/news/world/downer-defends-evacuation/2006/07/20/1153166495858.html)

Tim Chmielewski, Webmaster, Human Edge Software
<http://www.humanedge.biz> <<http://www.humanedge.biz/>>

⚡ Re: Yet another example of accidental disclosure of redacted info

<"Amos Shapir" <amos083@hotmail.com>>

Thu, 20 Jul 2006 18:32:55 +0300

(Emigh, [RISKS-24.34](#))

I once received a TIF file of a document that was exactly that: a scanned faxed image. But since the faxed printout was intended as a temporary step, the sender used the back side of old printed pages for that. When I noticed that the background of the sent TIF file was not completely white, it only took a few b&w enhancement steps in a graphics application, to clearly reveal what the sender did not intend to send!

There is even a risk in using blank paper for that, keeping in mind the "secret" yellow-dot identification code which is generated by many printers...

⚡ Re: Subject: Deceiving a computer is now a crime (Prevelakis, [R 24 34](#))

<"David H Smith" <d.smith@fnc.co.uk>>

Thu, 20 Jul 2006 09:07:50 +0100

> .. the attempt to attribute human characteristics to machines
> is bound to
> cause problems.

Er, not quite. The UK Government web site says

"Revised offence of obtaining services dishonestly (to fill a legal

loophole, since a machine cannot be 'deceived') with a maximum penalty of

five years' imprisonment."

<http://www.commonleader.gov.uk/output/page1221.asp>

Frazer-Nash Consultancy Limited, Stonebridge House, Dorking
Business Park,
Dorking, Surrey RH4 1HJ +44 (0) 1306 885050

🔥 REVIEW: "Insider Threat", Eric Cole/Sandra Ring

<Rob Slade <rMslade@shaw.ca>>

Mon, 10 Jul 2006 08:32:01 -0800

BKINSTHR.RVW 20060615

"Insider Threat", Eric Cole/Sandra Ring, 2006, 1-59749-048-2,
U\$34.95/C\$48.95

%A Eric Cole

%A Sandra Ring

%C 800 Hingham Street, Rockland, MA 02370

%D 2006

%G 1-59749-048-2

%I Syngress Media, Inc.

%O U\$34.95/C\$48.95 781-681-5151 fax: 781-681-3585 www.syngress.com

%O <http://www.amazon.com/exec/obidos/ASIN/1597490482/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/1597490482/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/1597490482/robsladesin03-20>

%O Audience n- Tech 1 Writing 1 (see revfaq.htm for explanation)

%P 397 p.

%T "Insider Threat"

Abuse of your systems by insiders, those who have intimate knowledge of an enterprise and its protective controls because they are either employees or close partners, has always been a great security risk. In most cases these people are aware of the existing safeguards, and usually some means to get around them: in a large number of situations inside people actually operate and manage security countermeasures and auditing functions. Protecting yourself against insider attack is tricky.

(However, while we all know about insider attacks, insider abuse, and that these are major problems, the term "insider threat" may be incorrect, and the phrase itself an obstacle. In viewing employees, staff, contractors, and partners as threats, instead of assets, we are making a serious mistake in our definitions, and one that can have serious negative consequences for the overall security of the enterprise.)

Part one examines insider threat basics. Chapter one points out that insiders are threats. Various technologies for carrying or hiding information are described in chapter two (although the text does admit that one possibility for info release is the fact your employees simply leave the building every night with everything they know).

Part two looks at government. Chapter three, about state and local authorities, notes the type of functions that are managed at this level, and the damage that can be done if this information is misused. The

material

seems to be bundled together in a random fashion. There are a number of "case studies," which are really just stories of situations where an insider has abused his or her position. Much the same is done with the federal government in chapter four.

Part three turns to corporations. Chapter five starts off with an extremely odd statement, seeming to imply that nobody was much aware of the insider threat until a 1998 study. (However, this may signal one of the major problems with the book: the term "insider threat" was first used in a classified paper in 1997.) It has a brief, but useful, examination of various types of damage that an insider can do in a commercial enterprise (sabotage, theft of intellectual property, theft of customer data, damage to reputation, and direct financial fraud), and then we are back to the stories again. More case studies are given regarding the banking and financial sector, in chapter six, and government subcontractors, in seven.

Part four is entitled "Analysis," but there isn't all that much. Chapter eight looks at profiles, despite the fact that the second last case study (in chapter seven) noted that the insider was so successful because he didn't fit the commonly perceived profile. The basic profile provided may be helpful in distinguishing low-end threats who may deserve further examination: the "high-end" profile identifies most senior managers. The responses suggested in chapter nine are primarily basic protections (and

mostly suitable for defending against outside threats); some of the additional measures are only effective if you already have a suspect. Most of the content in chapter ten relates to fundamental risk analysis.

The risks posed by insider knowledge are important. Unfortunately, other than providing a fund of illustrative stories, this book does not provide much material that would be of assistance to those concerned with protection. And, as noted previously, the title, and the general tone of paranoia pervading the work, are risks in themselves.

copyright Robert M. Slade, 2006 BKINSTHR.RVW 20060615
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>

REVIEW: "Practical VoIP Security", Thomas Porter et al.

<Rob Slade <rmslade@shaw.ca>>
Mon, 03 Jul 2006 09:41:29 -0800

BKPVOIPS.RVW 2060602

"Practical VoIP Security", Thomas Porter et al., 2006, 1-59749-060-1,
U\$49.95/C\$69.95
%A Thomas Porter
%C 800 Hingham Street, Rockland, MA 02370
%D 2006
%G 1-59749-060-1
%I Syngress Media, Inc.
%O U\$49.95/C\$69.95 781-681-5151 fax: 781-681-3585 amy@syngress.com

%O <http://www.amazon.com/exec/obidos/ASIN/1597490601/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/1597490601/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/1597490601/robsladesin03-20>

%O Audience i- Tech 2 Writing 1 (see revfaq.htm for explanation)

%P 563 p.

%T "Practical VoIP Security"

VoIP (Voice over Internet Protocol) is something of the new kid on the technology block, and computer folks may have limited experience with telephony. It therefore seems a bit strange that chapter one, as an introduction to VoIP security, starts out by talking about computer security and attacks. However, the structure of the book is rather odd in any case.

The basics of telephony, and the Public Switched Telephone Network (PSTN), are not covered until chapter four. Even then, while there is some useful

trivia, most of the content is a list of telephony protocols. Chapter three

covers some of the basic hardware and element information, discussing PBX (Private Branch eXchange) systems, VoIP components, and even power supplies.

That material, in turn, would be helpful to those who try to understand

chapter two, which is supposed to be about the Asterisk PBX software package. Although the text purports to deal with configuration and features

of Asterisk, most of the section's content covers PBX operations and

functions, dial plans, telephony numbering plans, and even a terse piece on

the vital aspect of circuit versus packet switching.

With chapter five, the book moves into some of the specifics of VoIP, discussing H.323, a protocol to specify data formats that is used extensively in commercial IP telephony products. SIP, the Session Initiation Protocol (used to negotiate interactive sessions over the net), gets a more detailed treatment (along with examination of related protocols) in chapter six. Other IP telephony architectures are briefly listed in chapter seven: the very popular Skype, H.248, IAX (Inter Asterisk eXchange), and Microsoft's Live Communications Server 2005 (MLCS). Diverse protocols used in support of VoIP are discussed in chapter eight. Most of these are commonly used in other Internet applications: some; such as RSVP (Resource reSerVation Protocol), SDP (Session Description Protocol), and Skinny; are more specialized. All the listed protocols have some review of security implications, which marks the first time in the book that security seems to be a major issue.

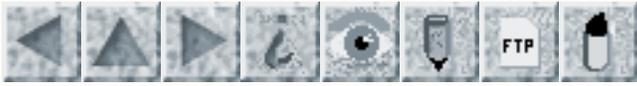
Chapter nine examines specific threats and attacks, mostly related to denial of service and hijacking. Securing the infrastructure used for VoIP is important, although the material in chapter ten is fairly standard information security. Chapter eleven reviews a number of ordinary authentication tools that are frequently used in VoIP. "Active Security Monitoring," in chapter twelve, is the traditional intrusion detection and penetration testing, and has nothing specific to IP telephony applications. Similarly, chapter thirteen examines normal traffic management

and LAN

segregation issues: the only telephony related content is in regard to VoIP aware firewalls. The IETF (Internet Engineering Task Force) has recommended certain existing security protocols in regard to IP telephony, and one addition (SRTP, Secure Real-time Transfer Protocol): these are outlined in chapter fourteen. Chapter fifteen lists various (United States) data security related regulations and the European Union privacy directive. The IP Multimedia Subsystem (IMS) structure is reviewed in chapter sixteen. Chapter seventeen repeats the recommendations made in chapters ten through fourteen.

It is handy to have a number of the issues related to VoIP addressed in one work. There is some depth to the content of the text as well, and those dealing with system internals may find that useful. However, for those who need to manage or make policy or purchasing decisions in regard to VoIP, this book may not have the forcefulness of complete analysis, or a structure that would assist in learning the background. While there is a considerable amount of helpful information, it reads more like an accumulation of miscellaneous facts than a directed study.

copyright Robert M. Slade, 2006 BKPVOIPS.RVW 2060602
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<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

Search RISKS using [swish-e](#)

Volume 24: Issue 36

Tuesday 8 August 2006

Contents

- [Electrical Fires in Queens](#)
[R. Mercuri](#)
- [AOL releases 500K users' search queries -- The Last Straw](#)
[Lauren Weinstein with included analysis by Seth Finkelstein](#)
- [Digital retouching of photos to make a propaganda point](#)
[Jeremy Epstein](#)
- [Voting machines in Ireland and The Netherlands](#)
[Erling Kristiansen](#)
- [Dutch energy company Eneco sends huge bill](#)
[Leon Kuunders](#)
- [Robot car park holds cars hostage](#)
[Steve Klein](#)
- [German road pricing system should help fighting crime, politicians say](#)
[Harald Vogt](#)
- [Unexpected consequences of airport random-screening glitch](#)
[Steve Summit](#)
- [RFID Clonable](#)
[Brad Malin via Dave Farber's IP](#)

- [Re: The Risks of retro computing?](#)
[Tom Watson](#)
 - [IEEE e-mail alias service with Comcast](#)
[Christopher Stacy](#)
 - [REVIEW: "Symbian OS Platform Security", Craig Heath](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Electrical Fires in Queens

<"R. Mercuri" <mercuri@acm.org>>
Mon, 24 Jul 2006 11:05:43 -0400

I don't know why the National news, or RISKS, isn't covering the electrical fires in Queens. There's been a series of power outages, exacerbated by fires that start off more fires. The news footage on NY TV stations is astonishing -- burning wires in the air, and explosions in manholes. The NY Times had an article at:
<http://www.nytimes.com/2006/07/22/nyregion/22cnd-power.html?hp&ex=1153627200&en=c53052af5d9b3841&ei=5094&partner=homepage>
and there's a community paper with a scary photo at:
http://www.zwire.com/site/news.cfm?newsid=16946439&BRD=2731&PAG=461&dept_id=574903&rfi=6
but otherwise there hasn't been much or consistent coverage by the major US media (see google news: electrical fires astoria), even though thousands have been without power, now for a week. Residents, business owners, and local leaders are becoming peeved at being ignored (including by Governor Pataki who's been refusing to declare the area a disaster).

[The outage lasted for about a week, but the aging underground

infrastructure is most likely still fragile and vulnerable to more such outages. Some of the wiring apparently dated to the beginning of the previous century. PGN]

✶ AOL releases 500K users' search queries -- The Last Straw

<Lauren Weinstein <lauren@vortex.com>>

Mon, 7 Aug 2006 09:55:15 -0700 (PDT)

Greetings. I've written and spoken many times about the sensitivity of search engine query data. We all know about Google's stance in DOJ vs. Google early this year, where Google wisely attempted (for several reasons) to prevent release of such data to a government fishing expedition related to "child protection" legislation. We also know that Gonzales, et al. are merrily pushing mandated data retention laws -- again mainly in the name of child protection -- that would leave Internet users vulnerable to all manner of unreasonable surveillance of their Internet activities. All of this is already enough to be sounding alarm bells regarding the lack of reasonable legislated protections for such data.

The AOL action in releasing the search records of a reported 500K AOL users -- assuming it took place as outlined below -- is probably the most egregious violation of users' search privacy in the history of the Internet, despite the half-hearted attempt at crude anonymization. The unbelievable

lack of responsibility or good judgment shown by AOL in this case should be enough to cause any remaining AOL subscribers (or users of their free services) to strongly consider ceasing any further contact with AOL.

Furthermore, we need to accept the fact that search query data is incredibly sensitive and often contains extremely personal data that does not lose its potential for abuse via simplistic forms of anonymization. Nor can we necessarily depend indefinitely on some individual search engines' honest and praiseworthy desires to protect such data (e.g. Google) in the face of intense competition and intrusive government actions.

Search query data can contain the sum total of our work, interests, associations, desires, dreams, fantasies, and even darkest fears.

We must demand that this data be protected.

--Lauren--

P.S.

I have removed URL reference (3) from the forwarded message below. Anyone who tried to forward that original message to an AOL user may have been in for a surprise.

At least in my experiments just now, AOL rejects that message since URL reference (3) contained a numeric IP address rather than a domain address.

Ironic, isn't it? AOL "protects" users by blocking messages with IP addresses in URLs (can such addresses be suspect? Yeah, but

they can easily
be legit, too) -- yet they happily release the most private
aspects of
users' search activities.

It's like a Fellini movie over there, but much less amusing.

Lauren Weinstein +1 (818) 225-2800 <http://www.pfir.org/lauren>
lauren@vortex.com or lauren@pfir.org Lauren's Blog: [http://](http://lauren.vortex.com)
lauren.vortex.com

From: Seth Finkelstein <sethf@sethf.com>
Date: August 7, 2006 1:05:50 AM EDT
To: Dave Farber <dave@farber.net>
Subject: AOL Releases Search Logs from 500,000 Users [From IP]

AOL Releases Search Logs from 500,000 Users
[1] Adam D'Angelo - 8/5/2006

AOL just released the logs of all searches done by 500,000 of
their users
over the course of three months earlier this year. That means
that if you
happened to be randomly chosen as one of these users, everything
you
searched for from March to May (2006) is now public information
on the
Internet.

This was not a leak - it was intentional. In their desperation
to gain
recognition from the research community, AOL decided they would
compromise
their integrity to provide a data set that might become often-
cited in
research papers: "Please reference the following publication
when using this
collection..." is the message before the download.

This is a blatant violation of users' privacy. The data is
"anonymized",
which to AOL means that each screenname was replaced with a
unique

number. "It is still a research question how much information needs to be anonymized to protect users," [9] says Abdur from AOL. Here are some examples of what you can find in the data:

User 491577 searches for "florida cna pca lakeland tampa", "emt school training florida", "low calorie meals", "infant seat", and "fisher price roller blades". Among user 39509's hundreds of searches are: "ford 352", "oklahoma disciplined pastors", "oklahoma disciplined doctors", "home loans", and some other personally identifying and illegal stuff I'm going to leave out of here. Among user 545605's searches are "shore hills park mays landing nj", "frank william sindoni md", "ceramic ashtrays", "transfer money to china", and "capital gains on sale of house". Compared to some of the data, these examples are on the safe side. I'm leaving out the worst of it - searches for names of specific people, addresses, telephone numbers, illegal drugs, and more. There is no question that law enforcement, employers, or friends could figure out who some of these people are.

I hope others can find more examples in the data, which is up for [10] download over here. The data set is very large when uncompressed which makes it pretty hard to work with, but someone should set up a web interface so people can browse it (or even 10% of it) without having to download the 400mb file. If you make a mirror or better interface to the data, or find other examples, let me know and I'll put a link up here.

This is the same data that the DOJ wanted from Google back in

March.

[11] This ruling allowed Google to keep all query logs secret. Now any government can just go download the data from AOL.

It's unclear if this is the type of data AOL released to the government

[12] back when Google refused to comply. If nothing else, this should be a good example of why search history needs strong privacy protection.

Thanks to Greg Linden for pointing this out [13] here.

Update 2: The md5 of the file AOL posted (and now removed) is 31cd27ce12c3a3f2df62a38050ce4c0a. I'm posting it so you can make sure you have a valid copy, but so far none of the copies I've seen are fake.

Update: Seems like AOL took it down. There are some mirrors of the data in the comments of the digg story, linked below. I estimate about 1000 people have the file, so it's definitely going to be circulated around. The [2] main AOL research page is still up, with some other data collections. The [3] google cache of the download page is still up, but you can't get the data. Here's discussion at other sites:

- * [4] siliconbeat
- * [5] techcrunch
- * [6] digg
- * [7] reddit
- * [8] zoli's blog

References

1. <http://www.ugcs.caltech.edu/~dangelo/>
2. <http://research.aol.com/pmwiki/pmwiki.php?n=Main.Home>
3. [removed to avoid AOL block]

4. http://www.siliconbeat.com/entries/2006/08/06/aol_research_exposes_data_weve_got_a_little_sick_feeling.html
5. <http://www.techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data/>
6. http://digg.com/tech_news/AOL_Releases_Search_Logs_from_500_000_Users
7. <http://reddit.com/info/cfvt/comments>
8. <http://www.zoliblog.com/blog/archives/2006/8/6/2204969.html>
9. <http://research.aol.com/pmwiki/pmwiki.php?n=Research.500kUserQueriesSampledOver3Months>
10. <http://research.aol.com/pmwiki/pmwiki.php?n=Research.500kUserQueriesSampledOver3Months>
11. <http://googleblog.blogspot.com/2006/03/judge-tells-doj-no-on-search-queries.html>
12. http://www.boingboing.net/2006/01/20/aol_we_did_not_compl.html
13. <http://glinden.blogspot.com/2006/08/chance-to-play-with-big-data.html>

Seth Finkelstein Consulting Programmer <http://sethf.com>
Infothought blog - <http://sethf.com/infothought/blog/>
Interview: <http://sethf.com/essays/major/greplaw-interview.php>

✦ Digital retouching of photos to make a propaganda point

<Jeremy Epstein <jeremy.epstein@webmethods.com>>
Mon, 7 Aug 2006 11:50:15 -0700

Digital retouching of photos isn't unusual, whether to make a teenagers acne go away or to make a joke. It gets serious though when it's used for propaganda.

Reuters yesterday withdrew photos that purported to show smoke rising from

buildings in Beirut after an Israeli bombing. After bloggers showed obvious evidence of tampering (such as buildings repeated through a picture, smoke that's duplicated), Reuters investigated and admitted that "photo editing software was improperly used on this image". They have now suspended the photographer. There are allegations by bloggers of other image tampering by the same photographer, Adnan Hajj.

<http://www.ynetnews.com/articles/0,7340,L-3286966,00.html>

describes the Reuters action. <http://littlegreenfootballs.com/weblog/> is one of the blogs that first reported the Photoshopping.

Certainly not the first time there's been distortion in time of war; the ease of manipulations combined with the power of bloggers to reveal what's going on may be part of a balance of power.

Voting machines in Ireland and The Netherlands

<Erling Kristiansen <erling.kristiansen@xs4all.nl>>

Fri, 21 Jul 2006 22:20:30 +0200

According to EDRIGRAM, the on-line newsletter of "European Digital Rights", number 4.14:

On 4 July 2006, the Irish Commission on Electronic Voting released its second report on the secrecy and accuracy of the e-voting system purchased by the Irish Government.

The summary remarks at the beginning of the 200 page report say:
"The
Commission concludes that it can recommend the voting and
counting equipment
of the chosen system for use at elections in Ireland, subject to
further
work it has also recommended, but that it is unable to recommend
the
election management software for such use."

The "further work" includes, among others:

- 1) add a voter verified audit trail;
- 2) replace the election management software (which prepares
election
data, reads votes from "ballot modules", and calculates
results) with a
version that is developed to mission critical standards;
- 3) modify the embedded software within the voting machines to
bring it
up to mission critical standard;
- 4) make certain modifications to the machines themselves;
- 5) test all components to mission critical standard;
- 6) modify the specification for the PC that is to be used for
vote management;
- 7) test the system as a whole (including end-to-end testing) to
mission
critical standard;
- 8) rectify the security vulnerabilities identified in the way
data is
transferred within the system.

This is quite a mouthful. In particular, the "mission critical
standards"
may be quite difficult to achieve as a retrofit. The article
speculates
that the responsible minister, who declares his intention to
continue the
project, "may not realize the extent of the changes required".
[Or is it a
polite way of saying "No thank you"? -EK]

Full article at <http://www.edri.org/edriagram/number4.14/>

[evotingireland](#)

The article includes several links, including a link to the full report.

As far as I can make out from various sources, the voting machines in question are essentially the same as the Nedap machines used in The Netherlands for years. Little public criticism of these machines appears in the general press.

But they do, indeed, have problems: According to the "Bits of Freedom" newsletter:

In a local election, one candidate got 1, 3, 7, and 181 votes, respectively, in the 4 polling stations where he was a candidate. The candidate not only was an election official in the high-vote station, he operated the machine!

Peter Knoppers, according to the article an expert on voting machines, is quoted saying that manipulation of the machine by a voting official is "a piece of cake". For example, if a key is turned at the exact moment of the vote being acknowledged by the voter, the vote will not be counted. The missed votes can then be added manually at a later time, for any candidate of your choice.

Full story (in Dutch) at

http://www.bof.nl/nieuwsbrief/nieuwsbrief_2006_14.html

This article also has several links, all in Dutch.

Dutch energy company Eneco sends huge bill

<Leon Kuunders <leon@kuunders.info>>

Tue, 25 Jul 2006 13:16:47 +0200

Apparently the Dutch energy supplier Eneco send an invoice for
**euro
2.144.607 and 90 cents [which in the US would be written as
2,144,607.90] to
a man for his two month energy usage. The man would have used
**20.000.000
kW electricity and 102.284 m3 gas.

When he called the energy supplier the call-center operator
replied with:

"It can be that this invoice isn't correct sir. We can sort it
out, but you
will have to pay the bill first. We can setup a payment
arrangement if you
like."

The cause of the error remains unknown.

Robot car park holds cars hostage

<Steve Klein <steveklein@mac.com>>

Tue, 8 Aug 2006 12:01:16 -0400

The city of Hoboken, New Jersey owns a parking garage with an
automated
car-parking system. The software that runs the hardware is
licensed from
Robotic Parking of Clearwater, Florida.

Following a recent contract dispute, the software license was
allowed to
expire and hundreds of cars were trapped in the garage for
several days.

More details here:

http://www.wired.com/news/technology/0,71554-0.html?tw=wn_index_1

Steve Klein, Your Mac Expert Phone: (248) YOUR-MAC or (248) 968-7622

German road pricing system should help fighting crime, politicians say

<harald.vogt@gmail.com>

4 Aug 2006 06:55:03 -0700

When the German Toll Collect system was put into operation in January 2005, it was accompanied by a law regulating the use of the data that is collected for billing. In particular, the system takes photographs of vehicles passing the scaffolds on which cameras and reading devices are mounted. According to this law, passing that information on to government agencies other than customs and the "Federal Agency for Commercial Transport" is illegal. This applies -- for now -- especially to the police, who cannot use the data for criminal prosecution. This is in accordance with German privacy regulations demanding that data collection has to serve a well-defined and well-stated purpose and cannot be done for future, yet unknown needs, such as not yet committed crimes.

It seems that a current case might turn that law upside down rather sooner than later. After an 18-year old female student was found dead

in a Autobahn parking lot, it became clear through DNA testing that the murderer is actually a serial killer who is wanted for a murder in 2003 and an attempted murder in 2004. As he is suspected to be a truck driver, the Toll Collect recordings may give a clue on his identity. However, the police is not allowed to get their hands on that data.

This case has sparked off a lively discussion in the political scene. Some (mostly right-wing politicians and police officials) say, the Toll Collect data should be used freely by police to investigate crimes. Others, such as data protection officers, reject that on grounds of data protection and privacy. As an obvious risk, they see the freedom of communication (which includes anonymous mobility) endangered by tendencies to promote surveillance. There are also some moderate voices who do not rule out the passing of data fundamentally but require high legal standards to do so. Members of the left-right coalition currently running the German federal government have announced to pursue a change in the aforementioned law that would allow to use the data for prosecution.

Apparently, police are currently trying to exploit a loophole in the system. While they are not allowed to use the Toll Collect data directly, police have asked shipping companies to look through their own files and report truck drivers that may have passed the parking lot during the night of the murder. If they comply, this would yield basically the same information to the police.

Interestingly, some politicians seem not so much concerned about the privacy of citizens, but rather whether there will be enough money left for building new roads after the Toll Collect infrastructure is extended into a surveillance tool. Today, the system is already very costly -- a quarter of the collected money is spent on its operation -- and would be even more if continuous surveillance was in operation. This money would then be lacking in the maintenance and building of roads. It seems the risk here is that a road surveillance tool could be created for which there exist no roads to monitor.

Unexpected consequences of airport random-screening glitch

<Steve Summit <scs@eskimo.com>>

Fri, 21 Jul 2006 17:52:45 -0400

This doesn't seem to have been covered in the media yet and I don't have full details, but according to an acquaintance who just traveled through there, a computer or computers unknown at Newark airport this morning (2006-07-21) mysteriously started selecting 20% of passengers for the random intensive security screening, instead of the normal 2%. No one felt authorized to countermand the computer's selections, so screeners were compelled to carry out all the excessive screenings, resulting in huge delays and many missed flights. A small glitch in a random

selection
process can have large and unexpected consequences.

⚡ RFID Clonable [From Dave Farber's IP]

<Brad Malin <b.malin@vanderbilt.edu>>

July 25, 2006 10:10:47 AM EDT

Hi Dave, remember a couple of years ago when you said you wanted to clone and repeat RFIDs - apparently someone has built the system to it.

-brad

<http://www.engadget.com/2006/07/24/verichips-human-implatable-rfid-chips-clonable-sez-hackers/>

VeriChip's human-implatable RFID chips clonable, sez hackers
Posted Jul 24th 2006 4:14PM by Donald Melanson
Filed under: Misc. Gadgets, Wireless

[Note: "implatable" is "mispelt" in both the URL and the title of the article, but the URL works as of when I am putting out this issue, and "implantable" is used in the text of the article! PGN]

In case anyone needed more proof that we're all living in a Philip K. Dick novel, a pair of hackers have recently demonstrated how human-implantable RFID chips from VeriChip can be easily cloned, effectively stealing the person's identity. Annalee Newitz and Jonathan Westhues showed off their handiwork at the HOPE Number Six conference in New York City this weekend, with Newitz herself playing the role of guinea pig, implanting a

VeriChip

RFID chip in her right arm. To clone the chip, Westhues first red Newitz's arm with a standard RFID reader, then scanned it again with a homebrew antenna connected to his laptop, which recorded the signal off the chip. He then used the same RFID reader to read the signal from his laptop, which promptly spit out Newitz's supposedly unique ID. For its part, VeriChip has only said they haven't yet had a chance to review the evidence but still insist that "it's very difficult to steal a VeriChip."

IP Archives at: <http://www.interesting-people.org/archives/interesting-people/>

Re: The Risks of retro computing? ([RISKS-24.35](#))

<"Watson, Tom" <t_wtom@qualcomm.com>>

Mon, 24 Jul 2006 11:34:55 -0700

The story mentions that the IBM 1401 computer "Can't Add Doesn't Even Try".

This is the wrong computer. The IBM 1620 is the computer that "Can't Add...". The computer museum has a working example. Later the IBM 1620, Model 2 could add, but still needed a table to multiply (but knew that multiplying by zero was a simpler operation). I can't vouch for the operations in the IBM 1401, as I haven't used the machine, but I am very familiar with the IBM 1620. Both machines hit the streets in the 1959-1960 time frame.

Not very Risks oriented, but a bit of history.

IEEE e-mail alias service with Comcast

<Christopher Stacy <cstacy@csail.mit.edu>>

Thu, 20 Jul 2006 19:36:02 -0400

Pete Klammer writes about losing email due to spam blacklisting due to the IEEE forwarding service's use of BrightMail. His analysis is that BrightMail is an "unaccountable third party" because IEEE could supposedly not obtain confirmation, logs, or rule sets describing the lossage of his messages.

But the other involved mail carriers, such as his ISP, IEEE, or even his own desktop software are all potentially filtering by using blacklist databases and rules which may be inscrutable. The problem is the unavailability of an audit trail.

The victimhood tone of the story and the suggestion that society is placing undue trust in third parties fails to identify a more straightforward accountability problem. His forwarding service (IEEE) has contracted with BrightMail for filtering services, but is then dismissing him when there's a problem with the forwarding service. This is simply poor customer service, and tantamount to "blaming the computer" as was very common in the 1970s. In the unlikely scenario that BrightMail customers cannot get

the necessary information, then what's happened is that IEEE made poor contract with that vendor. But I am pretty sure that BrightMail is not such a black box, and does indeed have the necessary audit trails. So the most likely explanation is that the IEEE folks were just too inept, lazy, or otherwise disinterested to bother accessing those resources when asked to investigate the problem.

This does not call for the elimination of a system in which third parties can be contracted for valuable email processing services. BrightMail is no more a "third party" in this scenario than IEEE. The risk is that if a computer is involved, people will accept lame blame-passing excuses from their various service providers.

🔥 REVIEW: "Symbian OS Platform Security", Craig Heath

<Rob Slade <rmslade@shaw.ca>>
Thu, 03 Aug 2006 10:44:52 -0800

BKSYOSPS.RVW 20060615

"Symbian OS Platform Security", Craig Heath, 2006, 0-470-01882-8,
U\$70.00/C\$90.99

%A Craig Heath

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 2006

%G 0-470-01882-8

%I John Wiley & Sons, Inc.

%O U\$70.00/C\$90.99 416-236-4433 fax: 416-236-4448

%O <http://www.amazon.com/exec/obidos/ASIN/0470018828/>

[robsladesinterne](#)

<http://www.amazon.co.uk/exec/obidos/ASIN/0470018828/>

[robsladesinte-21](#)

%O <http://www.amazon.ca/exec/obidos/ASIN/0470018828/>

[robsladesin03-20](#)

%O Audience a Tech 2 Writing 2 (see revfaq.htm for explanation)

%P 249 p.

%T "Symbian OS Platform Security"

Part one is an introduction to the Symbian mobile (cellular) phone operating system, and particularly its security provisions. Chapter one examines the reasons for the emphasis on security in a mobile phone: the users' perception of it as a more personal (and therefore more trusted) device and the acceptability of remote network installations and administration. Therefore, the developers of Symbian were faced with the challenge of creating an "open" development platform, while implementing security constraints. "Platform Security Concepts," in chapter two, presents an interesting basic catalogue, but concentrates on capability lists. (In this, the term may not be used in a standard manner: the capabilities appear to be preset, rather than being taken from the calling capability.)

Part two looks at application development for platform security. Chapter three describes the basic functions of the Symbian security environment. A decent, basic list of suggestions for writing secure applications is in chapter four, but there are few details. How to write secure servers (common processes), in chapter five, provides only generic advice, and has oddly little information that is distinctive to Symbian.

Chapter six, on the development of plug-ins, is more code and architecture specific. The safe sharing of data, in chapter seven, is addressed with a useful list of threats and countermeasures, and an outline of various security related components and provisions.

Part three deals with the management of platform security attributes.

Chapter eight examines the native software installer, concentrating on encryption key certificates. How developers obtain and use these certificates is reviewed in chapter nine. Some of the public key infrastructure behind the system can be inferred from the description (by those familiar with the concepts) but little detail is provided.

Part four, on the future of mobile device security, consists of chapter fourteen, which mentions a variety of potential functions for mobile phones.

For those wanting an introduction to the security provisions of the Symbian operating system, this work provides a useful starting guide. Developers, however, may need a bit more. For example, the statement is made that the platform is "less prone" to buffer overflows, but there is no discussion of why this is so, how it is achieved, or to what extent a developer can rely upon the operating system to protect against the problem of buffer overflows (or other types of malformed data). Given that most Symbian security is based on capability tables and certificates (and particularly with a somewhat non-standard definition of capabilities) these concepts, and their limits, should probably be explained more fully.

copyright Robert M. Slade, 2006 BKS Yosps.RVW 20060615
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<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

Search RISKS using [swish-e](#)

Volume 24: Issue 37

Saturday 12 August 2006

Contents

- [Letter on cybersecurity from Senator Reid to the President](#)
[PGN](#)
- [Survey on putting electronics in checked airline baggage](#)
[Lauren Weinstein](#)
- [More on medical errors](#)
[PGN](#)
- [RFID Guardian](#)
[Erling Kristiansen](#)
- [Search Engine Privacy - Re: AOL gaffe draws Capitol Hill rebuke](#)
[Lauren Weinstein](#)
- [LA power outages?](#)
[Dan Jacobson](#)
- [Your Cable Company -- powered by the guy with the extension cord](#)
[Lauren Weinstein](#)
- [Most college students vulnerable to cybercrime](#)
[Al Macintyre](#)
- [3.1 million HSBC](#)
[Al Macintyre](#)

- [Re: IBM 1620 - the joys of using punched cards](#)
[Chris Brady](#)
 - [REVIEW: "Frauds, Spies, and Lies", Fred Cohen](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Letter on cybersecurity from Senator Reid to the President

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

Fri, 11 Aug 2006 20:25:21 PDT

[Thanks to Marcus H. Sachs for this one.]

August 11, 2006
President George W. Bush
The Western White House
Crawford, TX 76638

Mr. President,

I write with deep concern over the lack of attention your Administration continues to demonstrate for computer and cyber security in the federal government.

Repeated failures at numerous government agencies have caused the disclosure of the personal or medical information of government employees, members of the military, veterans, and ordinary Americans. Your Administration has not seen fit to respond, however, and for the last year the position of Assistant Secretary of Homeland Security for Cyber Security has remained vacant. In fact, the previous official in charge of cyber security resigned in protest due to your Administration's persistent failure to

attend to this critical security issue. Shockingly, the acting Assistant Secretary has been a lawyer with no background in computer security who has questionable business ties to institutions that do business with the office he is supposed to manage.

Yesterday, the Department of Transportation reported that a laptop containing the personal information of approximately 133,000 drivers and pilots has gone missing. Three days ago, the Department of Veterans Affairs reported that it had lost a computer with the personal information of as many as 38,000 veterans. These disclosures come on the heels of previous failures at the VA that put the information of 26.5 million active duty, reserve, and retired military at risk. Over the course of your Administration, similarly grievous cyber security failures have occurred at the State Department, the FBI, the Energy Department, the Agriculture Department, the Federal Trade Commission, the Department of Health and Human Services, the Department of Defense, with our military in Afghanistan, and in the United States Navy.

This level of insecurity is unacceptable, and your Administration's repeated failure to correct the problem must cease. To that end:

* 1. Why has the position of assistant secretary of homeland security for cyber security not been filled, and what steps are you taking to ensure that it will be appropriately staffed at the soonest possible time?

- * 2. What administration-wide reviews are you undertaking and administration-wide guidelines are you instituting to ensure these repeated failures do not continue?

- * 3. What studies have you directed your administration to undertake to ensure that all previous data disclosures and security breaches are accounted for, and that the damage caused by each is minimized?

As we approach the fifth anniversary of September 11th, 2001, it is critical that the American people trust that their government is taking every possible step to protect them. Given the continued threat of al Qaeda and international terrorism and the volume of important personal and other information held by the federal government, your administration's cavalier attitude toward cyber security cannot continue. The security of the American people demands a new direction.

I hope you will direct your administration to answer these questions quickly and thoroughly, and will give the security of American people the attention it deserves.

Sincerely,
Harry Reid
Senate Democratic Leader

[This really **should** be a nonpartisan issue. Perhaps there is a similar message from a Republican? PGN]

Survey on putting electronics in checked airline baggage

<Lauren Weinstein <lauren@vortex.com>>

Fri, 11 Aug 2006 21:06:54 -0700

[Please distribute widely, as considered appropriate]

I'm conducting a little unscientific survey on whether or not airline passengers are willing to place their expensive or important electronic equipment in airline checked baggage (whether "locked" or not, but on most flights unlocked will be required), and how this would affect their flying patterns.

With the above as preface, there are three questions:

- 1) Are you willing to place all of your significant electronic equipment (including laptop or other computers, cellphones, DVD players, iPods, etc.) in checked baggage for airline flights?
- 2) If you are required to place such electronic equipment in checked baggage, would it have a significant negative impact on your willingness to fly?
- 3) Do you mainly fly for business or pleasure?

I will only publish aggregated statistics from this survey, unless individual persons specifically note that their responses may be released publicly.

To participate in the survey, please e-mail a note (or simply forward this message) with your responses to:

baggage@vortex.com

Only a one word reply is necessary to each of the questions unless you wish to add comments, which are invited.

Thanks very much.

Lauren Weinstein

lauren@vortex.com or lauren@pfir.org

Tel: +1 (818) 225-2800

<http://www.pfir.org/lauren>

Co-Founder, PFIR

- People For Internet Responsibility - <http://www.pfir.org>

Co-Founder, IOIC

- International Open Internet Coalition - <http://www.ioic.net>

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

Member, ACM Committee on Computers and Public Policy

Lauren's Blog: <http://lauren.vortex.com>

DayThink: <http://daythink.vortex.com>

More on medical errors

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

Sat, 22 Jul 2006 17:23:04 PDT

A major study lists confusion over names and wrong doses among the mistakes, and urges more use of computers in prescribing drugs.

At least 1.5 million Americans are injured or killed every year by medication errors at a direct cost of billions of dollars, according to a report issued Thursday by the prestigious Institute of Medicine in Washington, D.C.

For hospitalized patients, the report said that on average, one medication error per day was caused by confusion in drug names, wrong doses, failure to deliver drugs or a host of other problems.

The study is a follow-up to a 1999 report from the institute, which is part of the National Academies, that outlined all medical errors and claimed that as many as 98,000 people were killed each year as a result of medical errors -- 7,000 of them as a result of medication errors. The study lays out a detailed series of recommendations for new procedures and research to minimize the risk of future medication errors, emphasizing computerization of prescribing and administering drugs and data acquisition.

[Source: Medication Errors Hazardous to Your Health, Thomas H. Maugh II, *Los Angeles Times*, 21 Jul 2006; PGN-ed, tnx to Lauren Weinstein]

<http://www.latimes.com/features/health/la-sci-drugs21jul21,0,5771929.story?coll=la-home-health>

RFID Guardian

<"Erling Kristiansen" <erling.kristiansen@xs4all.nl>>
Wed, 9 Aug 2006 14:12:49 +0200 (CEST)

According to
http://www.bof.nl/nieuwsbrief/nieuwsbrief_2006_16.html (in Dutch)

Vrije Universiteit in Amsterdam, The Netherlands, has developed a prototype of a device capable to:

- Detect all RFID chips and scanners in its neighbourhood;
- Keep an inventory of all RFID chips you carry on your person, and alert you to new additions to the "inventory";

- Block the reading of any RFID you carry;
- Spoof a given RFID.

More details at <http://www.rfidguardian.org/> (in English)

✶ Search Engine Privacy - Re: AOL gaffe draws Capitol Hill rebuke

<Lauren Weinstein <lauren@vortex.com>>

Thu, 10 Aug 2006 09:14:32 -0700

Ladies and Gentlemen, Boys and Girls:

Web site privacy issues in general, and search engine privacy concerns in particular, are turning into a three-ring circus of ironies.

I discuss these issues until I'm figuratively blue in the face and yet it's deja vu over and over again.

The article referenced below in fact failed to mention the key aspect of the search engine data situation that makes this all so bizarre. We have Rep. Markey, et al., pushing data destruction laws in the wake of DOJ's push (in support of their Child Online Protection Act case) to get Google's query data -- which Google wisely resisted, though ultimately they had to turn some of that data over to DOJ. I do agree with some observers who feel that Markey's proposal is so encompassing that it remains unlikely to ever become law -- I'd much prefer to see more highly targeted and focused legislation.

But meanwhile, as some of us had been predicting for ages, DOJ/

Gonzales are out there pushing for broad Web site data *retention* laws -- ostensibly (do we see a pattern emerging?) using child abuse investigations as the hook.

Gang, we can't have it both ways in any kind of simplistic scenario. The simple choices are (1) Burn the data to prevent abuse -- and also prevent any other non-abusive uses of that data, or (2) Retain the data, along with major internal and external abuse potentials.

The simplistic scenarios are each highly problematic. We need to advance these issues in more sophisticated directions.

The only research and policy paths I see that could possibly lead toward better outcomes in this area are being largely ignored by the major players, so we have this repeating cycle of events and reactions banging back and forth.

A few months ago, in: "An Open Letter to Google: Concepts for a Google Privacy Initiative" (<http://www.vortex.com/google-privacy-initiative>) I set forth a proposal urging Google, as the global search leader, to apply its formidable resources toward advancing these issues -- both for Google's own benefit and ultimately for the benefit of the entire global community. In light of the whole series of recent events relating to the Web site data retention/destruction sphere, I assert that such efforts are needed now, on a priority basis.

As I've noted previously, we must demand that our data be

protected.

Accomplishing this properly requires serious thinking, hard work, and in the real world more than a little compromise. We need to develop effective and reasonable technology and policy paths toward management of the vast amounts of personally-related data that Web sites are collecting. AOL's search query data screw-up is bad enough, but it's only a drop in the bucket compared with the sorts of abuses and problems that could take place if we don't move forward appropriately. We can be enriched by data, or we can be enslaved by it. The choice remains ours.

Lauren Weinstein +1 (818) 225-2800 <http://www.pfir.org/lauren>
Lauren's Blog: <http://lauren.vortex.com> DayThink: <http://daythink.vortex.com>

⚡ LA power outages?

<Dan Jacobson <jidanni@jidanni.org>>
Thu, 10 Aug 2006 03:47:22 +0800

[My web provider has reassured me that the LA power outages are no risk:]

World class first tier facility, two redundant grid hookups, backup battery array with two separate sets of diesel generators. Trucks full of diesel are on standby and the datacenter is run on each for 12 hours each month to make sure everything is working as it should.

There's more: 24/7 armed security on premises, perimeter badge

required +
biometric hand scanners at the steel doors to each suite, locked
cages in
each suite and video cameras recording throughout with video
archived for 30
days. You can't even get into the front door of the building
without
clearance and ID which is logged.

Very early smoke detection systems as well as privately lit
fiber directly
into the meet me room at One Wilshire (over 200 of the worlds
first tier
providers connect to each other in that room).

This is *very* expensive space... even the power comes at a
pretty penny
since it is fully backed up power not just plain municipal.

This is something I rail about constantly because there is no
shortgage of
competition out there on municipal power with a single homed
local loop into
an office somewhere who can obviously beat me on price because
they don't
have any of this. And explaining all of this to people is
seemingly
impossible sometimes.

In short: at least for now, we're good. :-) You're right though
the AC units
are wreaking havoc here right now - it got up to 90 degrees
Fahrenheit!! Us
Southern Californians can't handle that any more than we can
handle half an
inch of rain! The AC units are flying off the shelves. It's a
feeding
frenzy! ; -)"

Dan Jacobson wrote:

> News has it that there are LA power outages.
> Certainly you have prepared bicycle and rodent wheel
generators?

> "Global warming kills information age."

⚡ Your Cable Company -- powered by the guy with the extension cord

<Lauren Weinstein <lauren@vortex.com>>

Sat, 12 Aug 2006 03:45:41 -0700 (PDT)

Last night at around 2:15am (yup, everyone's just leaving the bars) my area had a widespread power failure when someone wrapped themselves around a main distribution line power pole (this is a Friday and Saturday night tradition of course). While LADWP started on it pretty quickly, power was not restored for around seven hours.

That long an outage is enough to expose one of the serious weak points in our telecom networks -- remotely situated batteries. They don't last very long without external charging power, and we already know that microcell sites tend to go down quickly for this reason when power fails.

Early this morning when I started walking the area to see the effects, I quickly found an unmarked white bucket truck with engine running, parked at a nearby corner, with an orange extension cord running from its open hood to the open cable backup power box on the nearby pole, containing what looked like about three gel cells.

When I went over and talked to the friendly cable guy splicing wires on the

back of his truck, he told me that he wasn't even trying to charge the batteries, all he could do was try to keep the system running from his truck until power was restored.

Cable modems? Cable VoIP? Our whole world of modern cable telecom, dependent on a guy with an extension cord and an old bucket truck.

I found it rather amusing, in a "sad commentary" sort of way.

+1 (818) 225-2800 <http://www.pfir.org/lauren>

Lauren's Blog: <http://lauren.vortex.com> DayThink: <http://daythink.vortex.com>

⚡ Most college students vulnerable to cybercrime

<Al Mac <macwheel99@sigecon.net>>

Thu, 10 Aug 2006 13:47:32 -0500

<http://daily.stanford.edu/article/2006/8/10/thievesPhishForStudents>

A CompUSA survey of US college students

- * 88% keep on their computer desk tops and laptops the kind of info that could get their identity stolen if that computer was stolen or broken into
- * 41% ignorant of the concept of phishing
- * 21% had been tempted to give personal private info to web sites where they unsure of the security or of the source of the request for their personal data
- * 9% had already responded to phishing e-mails

There was an incident with Stanford's Axxess system, where a student's account was cracked, then someone else opened credit in the student's name, intercepting that student's money. That case has been solved.

> Increased cases of identity theft have led the Office of the Inspector General at the U.S. Department of Education to establish a Web site, www.ed.gov/misused, dedicated to informing students and parents about identity theft. Victims of identity theft can contact the Office of the Inspector General's Identity Theft hotline at 1-800-MIS-USED. Additionally, the Stanford Residential Computing Security Web site is available at <http://rescomp.stanford.edu/info/security>

Should students have billing sent home, rather than to a school address

whose mail system may be less secure?

Are cell phones locked up when not being used?

How often do you change passwords, PIN#s?

Do you know how your financial institutions contact you, so you can

recognize a fraudulent contact?

Do you know which institutions are brain dead on security, so you should

avoid doing business with them at all?

<http://daily.stanford.edu/article/2006/8/10/thievesPhishForStudents>

3.1 million HSBC

<Al Mac <macwheel99@sige.com.net>>

Thu, 10 Aug 2006 13:31:18 -0500

[http://www.thisismoney.co.uk/news/article.html?
in_article_id=411576&in_page_id=2](http://www.thisismoney.co.uk/news/article.html?in_article_id=411576&in_page_id=2)

Millions of customers, with one of Britain's biggest banks, exposed to on-line attack. The bank says the loophole can only be exploited by sophisticated attackers, while critics talk about how easy it is for troublemakers to get at the tools to do so.

This incident also illustrates a problem in ethics for computer security researchers. If you find a flaw, who should you report it to?

- * The institution with the flaw
- * Law enforcement
- * Only those who subscribe to your service
- * Publish some research document
- * The general news media

If you report it to the institution and to law enforcement, and they do not seem to take you seriously, you also have a responsibility to the potential victims NOT to be telling the news media, who in turn also guide cyber criminals to exploit the flaw. If this is not easy for people to understand, put it in terrorist terms ... you observe a flaw at an airport, in other transportation, that a terrorist could exploit to kill a staggering number of people. You tell the authorities and they ignore you. If you tell the news media, you may be giving ideas to criminals that they might not otherwise have figured out on their own.

⚡ Re: IBM 1620 - the joys of using punched cards

<Chris Brady <chrisjbrady@yahoo.com>>

Fri, 11 Aug 2006 11:12:53 +0100 (BST)

With regards to the IBM 1620 - Loughborough University (UK) had one in the late 1960s / early 1970s - and it was my very first introduction to a real computer - a step up from the electrical mechanical adding up machines we had to use in the Numerical Analysis course. For my fourth year final computer project I had written a sophisticated program in Fortran 2D on hundreds of punched cards that plotted the contours of 3D graphs of complex mathematical functions. An early fractal program I guess.

The IBM line printer used was exactly that with 200+ metal disks with the printing characters on 'teeth' around the edges. They all spun round to print an entire line at once - the whirring and clunking noise was horrendous.

Anyway in on graduation day my parents, assorted relatives and my younger brother (then aged 11) attended my degree ceremony. Afterwards, during a tour of the campus, I tried to demonstrate my 'fractal' program that I'd spent many weeks preparing. It didn't work. It wouldn't even compile. It misread almost every card with a syntax error - which was labouriously output on the operator's old-fashioned typewriter a character at a time.

It was only a few years ago that my uncle told me that whilst my back was turned my dear brother had shuffled some of the cards to see

what would
happen. Of course the cards weren't numbered so re-ordering them
wasn't an
option at the time.

The risk: never let anyone near your stack of punched cards -
especially
inquisitive brothers. P.S. My brother is now a famous computer
graphics
visualiser / illustrator for clients designing new buildings and
landscapes.
Now he has more laptops than I have.

REVIEW: "Frauds, Spies, and Lies", Fred Cohen

<Rob Slade <rmslade@shaw.ca>>
Thu, 10 Aug 2006 09:30:41 -0800

BKFRSPLI.RVW 20060710

"Frauds, Spies, and Lies", Fred Cohen, 2005, 1-878109-36-7, U
\$29.95/C\$33.45

%A Fred Cohen Fred.Cohen@all.net

%C 572 Leona Dr, Livermore, CA 94550

%D 2005

%G 1-878109-36-7

%I Fred Cohen and Associates

%O U\$29.95/C\$33.45 925-454-0171

%O [http://www.amazon.com/exec/obidos/ASIN/1878109367/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/1878109367/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/1878109367/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/1878109367/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/1878109367/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/1878109367/robsladesin03-20)

%O Audience n+ Tech 1 Writing 2 (see revfaq.htm for
explanation)

%P 234 p.

%T "Frauds, Spies, and Lies: and How to Defeat Them"

Over the years, lots of books have promised to teach us how to deal with social engineering, fraudulent practices, con jobs, deceit, and just plain old lies. There are the pedestrian warnings that it is dangerous out there, such as Barrett's "Bandits on the Information Superhighway" (cf. BKBOTISH.RVW). Or Mintz' listing of nasty Websites in "Web of Deception" (cf. BKWBDCPT.RVW). Or the repetitive recounting of confidence games in Mitnick and Simon's "The Art of Deception" (cf. BKARTDCP.RVW). Generally these works retail similar stories, with little variation and even less analysis.

Cohen's slim volume is a bit different.

Chapter one is a brief introduction to the structure of the book. Chapter two defines frauds, and then lists a huge series of variations on the theme. Many books that deal with the topic provide examples, but this exhausting (and nearly exhaustive) catalogue, even with minimal analysis, allows the reader to begin to see patterns and thus furnishes a useful alert for awareness of the issues, regardless of the student's background. (Fred, I wonder if you are entirely correct about 419 frauds.) The topic of deception, in chapter three, deals first with how we think, and what analytical mistakes we are likely to make. This preparation is augmented by examples of how fraudsters and confidence tricksters can use these errors. (An interesting addition is a section dealing with self-deception, in regard to the justifications scammers use.) Cohen's wit and humour are

used to
good effect in pointing out the absurdities of some of our
thinking
patterns. Most "spying" is not James Bond derring-do, and
chapter four
outlines the means that "HUMINT" (human intelligence)
specialists use to
obtain information, mostly in normal conversation. This
material would be
very useful in creating security awareness courses dealing with
social
engineering. Defence and counterintelligence is covered in
chapter five.
Chapter six leans more towards the countering of various types
of frauds.

This is not your normal security book, but then typical security
works have
had remarkably little success in addressing this particular
topic. Security
professionals will find little new in these pages, but the
aggregation of
the variant frauds is, itself, useful. Certainly no specialized
background
is needed to approach the text: anyone can pick it up and get a
good deal of
useful security awareness from a perusal of chapter two alone.
The size of
the work should not be daunting for anyone, and the content is
quite
readable. (I must note that the typography and formatting
creates a bit of
a problem: the lack of "white space" can sometimes make section
changes a
bit hard to follow, despite the careful and clear numbering of
sections and
subsections.)

I'd recommend this book, particularly as bedtime reading for any
security
professional, and for those involved with security awareness
programs.
However, it should have a broader readership: any reasonably

intelligent

person will find something useful and helpful for building a
safer and
enlightened attitude to the dangers of this complex world.

copyright Robert M. Slade, 2006 BKFRSPLI.RVW 20060710

rslade@vcn.bc.ca slade@victoria.tc.ca

rslade@computercrime.org

<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

Search RISKS using [swish-e](#)

Volume 24: Issue 38

Friday 18 August 2006

Contents

- [RFID car keys and insurance](#)
[Joshua Levy](#)
- [Anti-hijack software: what a great idea!](#)
[Nickee Sanders](#)
- [Bit bucket swallows 17 million AU dollars](#)
[Rodney Polkinghorne](#)
- [Sober Warnings About e-Voting Systems](#)
[Eric Sinrod via TechNews](#)
- [The FBI's Upgrade That Wasn't](#)
[Eggen and Witte](#)
- [Your Cable Company -- powered by the guy with the extension cord](#)
[Lauren Weinstein](#)
- [UK bank details sold in Nigeria](#)
[Amos Shapir](#)
- [Another auditor's laptop stolen](#)
[Neil Youngman](#)
- [First conviction in UK for Wi-Fi hijack](#)
[Peter Mellor](#)

- [Can't type? Your Dell laptop battery must be OK!](#)
[Dan Miller](#)
 - [Re: 3.1 million HSBC](#)
[Thor Lancelot Simon](#)
 - [Re: LA power outages](#)
[Scott Peterson](#)
 - [Re: Letter on cybersecurity from the president](#)
[Nick Simicich](#)
 - [REVIEW: "Risk Management Solutions ... Compliance, Quarterman](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ RFID car keys and insurance

<Joshua Levy <levy@csl.sri.com>>
Mon, 14 Aug 2006 09:46:30 -0700

[Source: Brad Stone, Pinch My Ride, *WiReD News*; PGN-ed]
http://www.wired.com/wired/archive/14.08/carkey_pr.html

To make a long story short, Emad Wassef had his Lincoln Navigator stolen from a Target parking lot in Orange County, California. He reported the theft to police and his insurance company. Two weeks later the SUV turned up near the Mexican boarder, stripped. His insurance company (Unitrin Direct) claimed the transponder antitheft system is absolutely nonspoofable. Brad Stone (the author of the article) himself had had a similar experience two years before, which he had written up for *Newsweek* in 2004, which led to many letters reporting similar thefts. Brad suggests various possibilities. Cloned key? Masquerader requesting a duplicate for an

observed vehicle identification number? He also discovered there is an emergency override known to insiders, involving a particular nongeneric sequence of mechanical actions. The moral of this story is that if you believe your transponder makes you more secure and less likely to get stiffed by your insurance company, forget about it.

✈️ **Anti-hijack software: what a great idea!**

<Nickee Sanders <njsanders@ihug.co.nz>>

Fri, 18 Aug 2006 18:15:10 +1200

A joint European effort is working on software that would enable remote control of an aircraft that could override any attempts by hijackers to control the plane, and force a safe landing. "The system would be designed in such a way that even a computer hacker on board could not get round it."

If successful, it would resolve various debates such as those going on in Germany about shooting down hijacked commercial airliners. The project is budgeted for 36m Euros. [Source: Yahoo News, 22 Jul 2006; PGN-ed]

http://news.yahoo.com/news?tmpl=story&cid=1509&e=10&u=/afp/20060722/tc_afp/germanyeuunrest

If only it were April Fools' Day...

Nickee Sanders, Software Engineer, Auckland, New Zealand

[Ah, perfect security at long last! How reassuring to RISKS readers. PGN]

✶ Bit bucket swallows 17 million AU dollars

<Rodney Polkinghorne <rodneyp@physics.uq.edu.au>>

Tue, 15 Aug 2006 14:49:28 +1000

Today's issue of **The Australian** has two stories about a new accounting system that Australian Pharmaceutical Industries installed when it outgrew Excel. The one in the IT section [1] features the company's information management leader congratulating himself on how quickly he got the new system got up and running.

The one in the business section [2] reports that the company's shares have been suspended from trading because the new books don't balance, and no one knows whether the company made 20 or 40 million Australian dollars last year.

[1] "Finding the right modelling tool", *The Australian*, 15th August 2006,

<<http://australianit.news.com.au/articles/0,7204,20098218%5E24170%5E%5Enbv%5E24169,00.html>>

[2] "API mystified by missing millions", *The Australian*, 15th August 2006,

<<http://www.theaustralian.news.com.au/story/0,20867,20129112-643,00.html>>

✶ "Sober Warnings About e-Voting Systems"

<TechNews <technews@HQ.ACM.ORG>>

Fri, 18 Aug 2006 16:29:02 -0400

[Source: Eric J. Sinrod, CNet (08/17/06) via ACM TechNews; 18 Aug 2006]

http://news.com.com/Sober+warnings+about+e-voting+systems/2010-1071_3-6106187.html

In its analysis of three of the most widely used electronic voting systems, the Brennan Center for Justice at New York University found significant security and reliability flaws in each of them that could compromise the integrity of local, state, and national elections. With sufficient precautions at the state and local levels, the most serious vulnerabilities can be addressed, but few jurisdictions have implemented the necessary countermeasures to shore up their systems. The study analyzed the Direct Recording Electronic (DRE) system, which directly records a voter's choices with a ballot that appears on the screen; DRE with Voter Verified Paper Trail, which captures the vote both electronically and on paper; and Precinct Optical Scan, which enables the voter to mark a ballot with a pen and then carry it to a scanner. It would be fairly easy for someone to deploy software attack systems to alter vote counts or launch an attack on the system with a wireless device. New York and Minnesota are currently the only two states that prohibit wireless components on all voting machines. The Brennan Center report recommends automatic, routine audits that compare electronic tallies with voter-verified paper records after every election. The report also urges states to adopt wireless bans and randomly

examine
machines on Election Day for viruses and worms.

✶ The FBI's Upgrade That Wasn't

<"Peter G. Neumann" <neumann@csl.sri.com>>
Fri, 18 Aug 2006 11:28:18 PDT

[Source: Dan Eggen and Griff Witte, The FBI's Upgrade That
Wasn't: \$170
Million Bought an Unusable Computer System, *The Washington
Post*, 18 Aug
2006, A01; PGN-ed]
[http://www.washingtonpost.com/wp-dyn/content/article/2006/08/17/
AR2006081701485_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2006/08/17/AR2006081701485_pf.html)

It was late 2003, and a contractor, Science Applications
International Corp
. (SAIC), had spent months writing 730,000 lines of computer
code for the
Virtual Case File (VCF), a networked system for tracking
criminal cases that
was designed to replace the bureau's antiquated paper files and,
finally,
shove J. Edgar Hoover's FBI into the 21st century. It appeared
to work
beautifully. Until Azmi, now the FBI's technology chief , asked
about the
error rate. Software problem reports numbered in the hundreds,
and were
multiplying as engineers continued to run tests. Scores of basic
functions
had yet to be analyzed. "A month before delivery, you don't
have SPRs,"
Azmi said. "You're making things pretty. . . . You're changing
colors."

[This is more on an old story that was foreordained a long

time ago. PGN]

⚡ Your Cable Company -- powered by the guy with the extension cord

<Lauren Weinstein <lauren@vortex.com>>

Sat, 12 Aug 2006 03:47:03 -0700

Last night at around 2:15am (yup, everyone's just leaving the bars) my area had a widespread power failure when someone wrapped themselves around a main distribution line power pole (this is a Friday and Saturday night tradition of course). While LADWP started on it pretty quickly, power was not restored for around seven hours.

That long an outage is enough to expose one of the serious weak points in our telecom networks -- remotely situated batteries. They don't last very long without external charging power, and we already know that microcell sites tend to go down quickly for this reason when power fails.

Early this morning when I started walking the area to see the effects, I quickly found an unmarked white bucket truck with engine running, parked at a nearby corner, with an orange extension cord running from its open hood to the open cable backup power box on the nearby pole, containing what looked like about three gel cells.

When I went over and talked to the friendly cable guy splicing wires on the

back of his truck, he told me that he wasn't even trying to charge the batteries, all he could do was try to keep the system running from his truck until power was restored.

Cable modems? Cable VoIP? Our whole world of modern cable telecom, dependent on a guy with an extension cord and an old bucket truck.

I found it rather amusing, in a "sad commentary" sort of way.

Lauren Weinstein +1 (818) 225-2800 <http://www.pfir.org/lauren>
Moderator, PRIVACY Forum - <http://www.vortex.com> Blog: <http://lauren.vortex.com>

⚡ UK bank details sold in Nigeria

<"Amos Shapir" <amos083@hotmail.com>>
Mon, 14 Aug 2006 18:17:22 +0300

Bank account details belonging to thousands of Britons are being sold in West Africa for less than £20 each, the BBC's Real Story programme has found. It discovered that fraudsters in Nigeria were able to find internet banking data stored on recycled PCs sent from the UK to Africa.

[<http://news.bbc.co.uk/2/hi/business/4790293.stm>]

⚡ Another auditor's laptop stolen

<Neil Youngman <neil.youngman@youngman.org.uk>>

Sun, 13 Aug 2006 17:12:56 +0100

Recently my wife received a letter from Ernst and Young, regarding the loss of a laptop containing credit card information for customers of various travel websites. I don't recall seeing it mentioned on RISKS, so I thought I'd add it to your collection.

The letter states that "For the past several years, Ernst and Young has been the auditor for IAN.com, a travel company which provides the hotel product and booking technology to many leading travel websites." ... "An Ernst and Young employee's backpack containing his laptop computer was stolen from his locked vehicle in the US." ... "Following the theft we commenced an internal investigation of this matter and determined that the stolen computer contained certain customer information regarding some IAN.com customer transactions primarily from the year 2004. There were also a small number of transactions from 2003 and 2002. We believe the transaction information may have included a transaction you made with IAN.com and, specifically, that the information on the laptop may have included your name, address and some credit or debit card information you provided. "

The laptop required a password to use it. To date we have received no information from law enforcement officials that any of the data stored on the computer has been accessed by an unauthorised person or used improperly. There is insufficient information in the letter for me to

determine which website was involved and which credit card might be affected.

Ernst and Young do say at the end "We have put in place enhanced security procedures, including encrypting our laptop computers, to provide additional protection for sensitive information and have taken other measures to designed to protect against this type of incident happening again."

⚡ First conviction in UK for Wi-Fi hijack

<MellorPeter@aol.com>

Sun, 13 Aug 2006 13:29:40 EDT

Quoted from BBC News article:

"A recent court case, which saw a West London man fined =A3500 and sentenced to 12 months' conditional discharge for hijacking a wireless broadband connection, has repercussions for almost every user of wi-fi networks.

It is believed to be the first case of its kind in the UK, but with an estimated one million wi-fi users around the country, it is unlikely to be the last. "There are a lot of implications and this could open the floodgates to many more such cases," said Phil Cracknell, chief technology officer of security firm NetSurity."

Apparently, the convicted man had used his laptop from his car while parked outside a house in which the resident was using an unsecured wi-

fi

connection, over a period of three months. Neighbours noticed him and reported his behaviour to the police as suspicious.

For the full article, see:

<http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/4721723.stm>

Peter Mellor; +44 (0)20 8459 7669 MellorPeter@aol.com (new)

⚡ Can't type? Your Dell laptop battery must be OK!

<"Dan Miller" <Dan.Miller@fastsearch.com>>

Tue, 15 Aug 2006 10:43:07 -0400

Dell has set up a website where you can check to see if your laptop battery is one of the group being recalled, due to overheating. See <https://www.dellbatteryprogram.com/batterymodels.aspx>

If your laptop belongs to a certain subset of models, you need to find your battery ID (printed on the battery itself). The code is of the format `zz-zzzzzz-zzzzz-zzz-zzzz`; a combination of 20 numbers and uppercase letters. If the last 5 characters of the second group match one of 36 combinations, you are directed to enter the entire ID to see if your battery needs replacement. See <https://www.dellbatteryprogram.com/Identify.aspx>.

The form in question allows you to enter one or more 20-character codes and hit a Submit button. If your battery is OK, the phrase "No need for replacement" appears next to the entered ID. I don't know what

it says if
your battery does need to be replaced.

Unfortunately, there appears to be absolutely no check to verify you entered a proper ID. Apparently, battery AB-CDEFGH-IJKLM-NOP-QRST is OK, as is 00-000000-00000-000-0000, and ten random combinations of numbers and letters.

So you'd better heed the warning at the bottom of the page to "Please verify you entered your PPID correctly before submitting". You can tell a zero from a capital letter O if only one of them appears on a label, right?

<http://www.nytimes.com/2006/08/14/technology/14cnd-battery.html?hp&ex=1155614400&en=499692c95b993103&ei=5094&partner=homepage>

[Of course, if you were injured in the process, you could call on the Pharma in the Dell. E-EYE-E-I-O. PGN!!!]

⚡ Re: 3.1 million HSBC (Macintyre, [RISKS-24.37](#))

<tls@panix.com (Thor Lancelot Simon)>
Mon, 14 Aug 2006 04:01:46 +0000 (UTC)

To be, perhaps, all too kind, the claim is nonsense, and the fact that its sole support is an argument about bombs at airports (which I've snipped) is good reason to suspect as much as soon as you see it. The "bomb" example is an exercise in emotional manipulation through the presentation of an

immediate, vivid, highly aversive consequence, intended to trick the reader into miscomputing the actual cost and benefit of the other problem it accompanies (the "telling the news media about a security flaw" problem) for emotional reasons.

To be clear, let's look at the actual ethical problem here in simple consequentialist terms. To believe that "you have a responsibility NOT to be telling the news media", you have to believe that the negative consequences of you telling the news media outweigh, for ever and ever going forward from today-here-now, the positive consequences of you doing so.

Is that really plausible? Absent the specious "bomb" example, why should we think so, when we have been given, as the conditions of the problem, that "you report it to the institution and to law enforcement, and they do not seem to take you seriously"? That suggests that (at least) whatever level of harm is currently occurring will continue indefinitely -- unless, that is, someone else were to make a public disclosure, and thus even more dramatically absolve you of this phantom 'responsibility' Al is claiming that you have. At some point in time, it is clear that the small continuing harm of continual abuse of the security flaw would in fact far outweigh the (allegedly) larger, very temporary harm of which your disclosure of the flaw to the media would purportedly be the cause -- after which disclosure, of course, all harm would stop, since fear of

liability would
cause the institution to plug the hole.

The correct choice as a matter of consequentialist ethics is plainly to continue to attract the correct attention from the appropriate authorities, but to be prepared to publicly disclose the problem before that small continuing cost swamps the one-time cost of disclosure. To claim that one has some kind of absolute responsibility to not disclose such problems as a matter of ethics is balderdash, and emotional appeals to examples about ticking bombs do not (as they usually do not) help.

✉ **Re: LA power outages (Jacobson, [RISKS-24.37](#))**

<Scott Peterson <scott4@mindspring.com>>
Sat, 12 Aug 2006 20:24:32 -0700

>World class first tier facility, two redundant grid hookups,
>backup battery
>array with two separate sets of diesel generators. Trucks full
>of diesel are
>on standby and the datacenter is run on each for 12 hours each
>month to make
>sure everything is working as it should.

I had a girlfriend who worked as a programmer for Carter Hawley Hale. This was a good sized California department store chain back in the 1980's. They built a huge data center in Orange County, CA. They made the same kind of plans for their mainframes.

Tied into multiple grids for power backup, got permission to use the cities fire hydrant water system for cooling as backup to the regular water supply. They thought they had everything covered. Anyway, one day a car hit a hydrant about a block away. A valve that was supposed to stop backflushing hadn't been installed properly and when the city tried to shut off the hydrant break they found that the datacenter was pumping water from the city lines into the emergency system with no way to shut it off without turning off water to the whole data center. They were down for about 4 days and it was pretty disastrous.

🔥 Re: Letter on cybersecurity from the president

<Nick Simicich <njs@scifi.squawk.com>>

Thu, 17 Aug 2006 10:18:27 -0400

After publishing this deprecation of the current administration from the loyal opposition, our moderator makes a weak call for "a similar message from a republican".

I have a further request: How about not publishing things that are obviously political diatribes masked as legitimate technical criticisms and comments?

It does bother me that the moderators seem to be unable to tell a polemic, complete with vague, denigrative suggestions from a legitimate technical criticism. I won't bother with a point by point response, that

would give
too much attention to a content-free political speech.

One thing does scare me about Reid's polemic. Toward the end,
flag firmly
in hand, he refers to 911 and then makes the following comment:

> it is critical that the American people trust that their
> government is taking every possible step to protect them.

No, every reasonable and constitutional step, not every possible
step. We
have already had a series of unreasonable steps, like no nail
clippers on
airplanes, and losing your items rather than having them mailed
or checked
through as punishment for accidentally bringing them (still in
effect).

The "every possible" language is tossed about by both sides, and
it is
tossed about by people who probably are not affected by either
the measures
they take or their results, short or long term. Yes, we are at
war, and at
war, you take some special actions. -- Blog:
<http://majordomo.squawk.com/njs/blog/blogger.html> Atom:
<http://majordomo.squawk.com/njs/blog/atom.xml> RSS:
<http://majordomo.squawk.com/njs/blog/atom.rdf>

REVIEW: "Risk Management Solutions ... Compliance, Quarterman

<Rob Slade <rMslade@shaw.ca>>
Thu, 17 Aug 2006 09:07:42 -0800

BKRMSOX.RVW 20060722

"Risk Management Solutions for Sarbanes-Oxley Section 404 IT

Compliance", John S. Quarterman, 2006, 0-7645-9839-2,
U\$50.00/C\$64.99/UK#31.99

%A John S. Quarterman

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 2006

%G 0-7645-9839-2

%I John Wiley & Sons, Inc.

%O U\$50.00/C\$64.99/UK#31.99 416-236-4433 fax: 416-236-4448

%O <http://www.amazon.com/exec/obidos/ASIN/0764598392/>

[robsladesinterne](#)

<http://www.amazon.co.uk/exec/obidos/ASIN/0764598392/>

[robsladesinte-21](#)

%O <http://www.amazon.ca/exec/obidos/ASIN/0764598392/>

[robsladesin03-20](#)

%O Audience a+ Tech 2 Writing 2 (see revfaq.htm for
explanation)

%P 278 p.

%T "Risk Management Solutions for Sarbanes-Oxley Section 404 IT
Compliance"

There is a problem with the title, quite apart from the fact
that it is just
too long. This book is not about "Sarbanes-Oxley Section
404" (which is in
the largest type on the front cover) as such. In the preface,
Quarterman
explains that this work addresses risk management, and,
specifically, those
risks related to the Internet. The text is intended for a wide
ranging
audience: C-level executives who need to manage and report risk,
IT
professionals needing information about non-technical control of
risk,
insurance and financial organizations needing to make monetary
assessments
of risks and benefits, employees of Internet related companies,
and business
risk management students.

Having been through the publishing process myself, I know that
the title and

cover are not Quarterman's fault: publishers get to choose. (And, somewhere in Wiley, there is a marketing person just bouncing up and down with glee at finally being able to publish a SOX book.) On the other hand, the title is not completely misleading: SOX 404 is about the proper assessment and reporting of potential risks, and pretty much every company these days has to factor in the perils of dependence upon the Internet.

Chapter one is an introduction, noting that, contrary to standard risk assessment ideology, some threats are beyond the control of the enterprise, and not subject to any kind of technical safeguards. Perils may be too large for the company (some financial losses are simply too great for an individual company to survive) and difficult to quantify. Quarterman points out that, rather than a fixed value resource, the Internet may be more similar in valuation to a stock option, or other financial instrument, and doesn't fit older cost/benefit models. A variety of hazards from and to the Internet are listed in chapter two. Solutions are addressed in chapter three, and the author also examines proposed solutions that do not work. For example, the difficulties of the Internet are frequently blamed on the fact that there is no central authority and management, and it has often been proposed to implement (or impose) such centralized command structures on the net. However, Quarterman demonstrates that decentralization has worked in a number of cases, including a number of Internet applications.

Chapter four, is problematic: options for risk transfer are discussed before the concept is raised, and although the title talks about strategy it is hard to pick strategic measures out of all the tactical measures. The work of Basel II, with the concepts of credit and operational risk calculations, are outlined in chapter five. Examples of risks that are troublesome to quantify are given in chapter six.

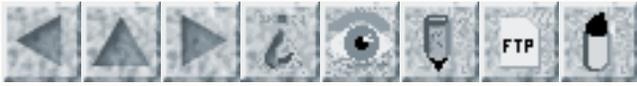
Chapter seven turns to large enterprises, noting some threats that are somewhat intrinsic to the breed. Quarterman doesn't stop with the "trite but true": some of the perils are hubris and a reputation for bullying behaviour. Small enterprises might not find the same kind of help in chapter eight: the material here talks more about opportunities and benefits. Various aspects of bonding, insuring, and service level agreements (SLAs) for Internet service providers are examined in chapter nine. There is an interesting discussion of third-party bonding, and the advantages that automatically accrue to all parties under such a situation. Chapter ten turns to the government, and the ways in which it can, and can't, help. Numerous aspects of insurance; policy language, legal precedents, new concepts, and the lack of hard data for the effectiveness of the new instruments; are reviewed in chapter eleven to address the possibilities, limits, and restrictions of new forms of risk transference. Chapter twelve summarizes the reasons why Internet risk is different than others.

This book has a rushed feeling to it, and there are a number of odd errors. The "Acknowledgements" section is, instead, a repeat of the first page of

the preface. Text and phrases are repeated ("cyberhurricanes"), often without definition and sometimes in contradictory fashion. There is, for example, an amount of \$100 billion for risk from the Internet. This number is repeated on pages xxiii, 1, 30, 146, and 256 but seems to be used in one place for a global figure, and in another for the risk to an individual company. The structure of individual chapters can be difficult as well: it is hard to determine threads of specific arguments out of the (admittedly intriguing) stream of information.

There are three threads that are repeated again and again in the book: diversity, insurance, and mapping of the Internet. But there is much more: Quarterman does not address the standard picture of risk management, since he is pointing out that the Internet throws our usual tools for quantified risk analysis into disarray. Instead he notes areas that have been neglected, because of the difficulty of fitting them into standard models, and proposes new, if somewhat vague, risk paradigms. This is not a text that can be used as a reference for ordinary threat analysis, but should be thoroughly studied by anyone involved with protecting information (and particularly communications) for a large company, anyone with a major involvement in the Internet itself, and anyone responsible for business risks in a rapidly changing environment.

copyright Robert M. Slade, 2006 BKRMSOX.RVW 20060722
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<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

Search RISKS using [swish-e](#)

Volume 24: Issue 39

Thursday 24 August 2006

Contents

- [Pull the Plug on Touchscreens](#)
[R. Mercuri](#)
- [Re: Pull the Plug on Touchscreens](#)
[Avi Rubin](#)
- [More on Diebold, Ohio, and Touchscreens](#)
[PGN](#)
- [Search Engine Privacy Dilemmas, and Paths Toward Solutions](#)
[Lauren Weinstein](#)
- [Centrelink staff busted invading Australians' privacy](#)
[David Shaw](#)
- [TiVo Is Watching When You Don't Watch, and It Tattles](#)
[Monty Solomon](#)
- [The SAFEE Project](#)
[Peter B. Ladkin](#)
- [Re: LA power outages](#)
[Kent Borg](#)
- [At least the extension cord worked](#)
[Mike Albaugh](#)

- [Re: ... Your Dell laptop battery must be OK!](#)
[Dave Blake](#) [Brent Kimberly](#)
 - ["IT Security Project Management", Susan Snedaker](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Pull the Plug on Touchscreens

<"R. Mercuri" <notable@notablessoftware.com>>

Tue, 22 Aug 2006 13:34:21 -0400

Forbes Magazine (9/4/6) included a commentary by Aviel Rubin where he complains about the "Help America Vote Act, which handed out \$2.6 billion to spend on voting machines." Avi's recent recommendation is that voters cast only optically scanned ballots that will be randomly audited. But does he go so far as to suggest that voters be allowed to prepare these ballots by hand? Absolutely not. Although I have publicly recommended the adoption of only scanned paper systems since at least 2003, Avi continues to recommend electronic ballot preparation methods, such as described in his Forbes piece, that require all voters to "make their selections on a touchscreen machine."

If humans are deemed capable enough to audit ballot counts, they should also be allowed to directly prepare their own ballots without the intervention of a computer. Most voters already do this, since some 60% of US counties and a steadily increasing number of mail-ins (such as in CA, FL and NJ where any

voter can register as a permanent absentee) use hand-prepared paper ballots. Sure, modern technology must be available to provide assistance for voters who need or want it, but this does not necessarily have to be limited to "touchscreen machines." Tactile ballots (endorsed by the United Nations, see <http://www.electionaccess.org/Bp/Ballot_Templates.htm>) and mechanical devices (such as the Vote Pad <<http://www.vote-pad.us/>>) offer inexpensive alternatives that do not require electricity.

So, will this advice help America's voters avoid the use of unreliable or insecure voting equipment in 2006, 2007, or even 2008? No, because purchases (costing in excess of \$5B, including state allocations and associated long-term service contracts) are already in place. Avi's change of heart (he's previously supported vote-tabulating DREs, see <<http://avirubin.com/vote/eac2.pdf>>) now favoring optically scanned ballots is simply too little, too late, and his ongoing endorsement of touchscreen voting has made him part of the problem, not its solution.

Rebecca Mercuri

✉ **Re: Pull the Plug on Touchscreens (Mercuri, [RISKS-24.39](#))**

<Avi Rubin <rubin@jhu.edu>>

Wed, 23 Aug 2006 13:42:21 -0400

I need to set the record straight on one point. Towards the end of

her posting, Rebecca states that

"[Avi has] previously supported vote-tabulating DREs, see avirubin.com/vote/eac2.pdf"

I urge anyone who is interested to have a look at what I wrote in my EAC testimony that she references. It is a scathing critique of DREs. I feel that accusing me of having supported DREs is like accusing Erin Brockovich of having supported water pollution. I have done nothing but argue and fight against DREs from day one. If you read my new book, *Brave New Ballot* (Random House, 2006), you will see that I have maintained a steady position on this all along.

Avi Rubin

🔥 More on Diebold, Ohio, and Touchscreens

<"Peter G. Neumann" <neumann@csl.sri.com>>
Wed, 23 Aug 2006 16:08:56 PDT

A report questioning the accuracy of Diebold Election Systems' e-voting equipment in a recent Ohio election gives more ammunition to critics who doubt the viability of electronic voting technology. A study of 467 of 5,407 e-voting machines used in the 2 May 2006 primary election in Cuyahoga County, Ohio, found that one-third of the booth workers had problems setting up the machines. 45% had problems closing out machines. 38% had problems with printers or spools. 90% of the voters liked the new

systems. 10% of the voters reported problems with the machines. [Source: Marc Songini, Paper Trail Flawed in Ohio Election, Study Finds *Computerworld*, 21 Aug 2006]
<http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyId=13&articleId=9002610>

✦ Search Engine Privacy Dilemmas, and Paths Toward Solutions

<Lauren Weinstein <lauren@vortex.com>>
Mon, 21 Aug 2006 21:51:46 PDT

An item in *The New York Times*, 22 Aug 2006 neatly encapsulates the overall state of search engine query data retention issues.
<http://www.nytimes.com/2006/08/22/technology/22aol.html>

The observant reader will note that despite the rising tide of concerns regarding search query privacy, the industry as a whole is still pretty much in a state of denial, made all the more confusing by various signals from the U.S. Department of Justice.

This is turning into such a mess that it's becoming difficult to even keep the various participants and their positions completely clear. There is every reason to believe that without heroic action by the players involved, we may be heading toward a privacy, legislative, and judicial nightmare. But maybe there's a way out.

Let's review:

AOL's release of search query data made obvious to everyone what many of us knew all along -- that such data contains all manner of personal information, even when the identity of the party making the query is not immediately known directly from usage logs. In the AOL case, the individual query entries were linked by "anonymized" user IDs, but even without such linkages the query items alone can be highly privacy-invasive. The AOL release triggered (as did DoJ vs. Google) broad calls for mandated search query data destruction policies.

The personal nature of the AOL query data serves nicely to liquidate the DoJ's arguments (again, as in DoJ vs. Google) that such data is not privacy-invasive so long as the query source is unidentified. The expressed DoJ reasoning in this regard is obviously faulty.

Search engine companies have been reluctant to voluntarily dispose of query data on a regular basis. This data has considerable R&D, marketing, and other value. Since the incremental cost of keeping all queries archived forever is so low, there is little incentive within the normal business structure to dispose of this resource, absent overriding considerations.

Even while laudably expressing concerns about the potential for third-party misuse of query data, search engine firms (e.g. Google) have proclaimed their intention to keep collecting and saving this data indefinitely. If AOL actually sets in place an aggressive data destruction schedule, it will be something of a watershed event that may (or may not) have

broad impacts

across the search engine industry. Fears of being placed at a competitive disadvantage will tend to make unilateral moves toward query data destruction difficult to propose or implement.

Meanwhile, DoJ is moving in exactly the opposite direction, apparently

preparing to propose long-term (perhaps measured in years) mandated data

retention schedules, requiring the saving of the very data for which

destruction demands are being made in other quarters. DoJ is using child

abuse (and as of late anti-terrorism efforts) as their hooks to justify such

legislation (please see: <http://lauren.vortex.com/archive/000186.html>).

This situation has all the elements of a painful and wasteful deadlock,

potentially triggering years of litigation while the overall search engine

issues continue to fester and become even bigger privacy,

business, and

political problems.

If we wish to avoid this scenario -- or at least have a good shot of

avoiding it -- we need to act now, and we need to do so cooperatively.

There are policy and technological approaches to the search query dilemma

that can be applied in ways that will serve the interests of all stakeholders. Cooperation and compromise mean that nobody is likely to get

everything that they'd ideally want, but to paraphrase the great philosopher

Mick Jagger, perhaps we can all get much of what we need.

Therefore, I propose the formation of a high-level Internet working

group/consortium dedicated specifically to the cooperative

discussion of these issues and the formulation of possible policy and technology constructs that can be applied toward their amelioration. Such a working group would be as open as possible, though proprietary concerns would likely necessitate some closed aspects if progress is to be accelerated as much as possible.

Participation by all stakeholders would be invited. Representatives of the major search engine firms and concerned government agencies, outside technologists and other persons involved in privacy and search issues, and other entities as appropriate would all play important roles.

Of course, it's easy -- especially for large corporate enterprises -- to simply ignore such efforts and just plow ahead independently. Obviously, without the participation of the key players, the effort that I'm proposing would be useless, and I will not continue to promote it if that situation ensues.

However, I suggest that it will be in the long-term best interests, both financially and in terms of corporate and organizational responsibility, for major stakeholders to actively join such a project, since the alternative seems ever more likely to be somewhere between highly disruptive and extremely draconian.

Interested? Please let me know. All responses will be treated as confidential unless the sender indicates otherwise.

Thank you for your consideration.

Lauren Weinstein <lauren@vortex.com> +1-818-225-2800 <http://www.pfir.org/lauren>

Lauren's Blog: <http://lauren.vortex.com> Co-Founder, PFIR <http://www.pfir.org>

Centrelink staff busted invading Australians' privacy

<"Shaw, David \ (David\)" <dshaw@avaya.com>>

Wed, 23 Aug 2006 10:31:06 +1000

Centrelink (www.centrelink.gov.au) is the Australian federal government's social security and welfare agency. Staff have access to a wide range of information about Australians.

Following a two-year investigation nineteen staff have been sacked for inappropriately accessing the personal information of family, friends and ex-lovers. More than 100 staff resigned when confronted with similar allegations. Five cases have been referred to the Australia Federal Police. The privacy invasions were detected using "specially designed spyware software."

While highlighting the risk that sometimes the greatest security threats come from within, at least it's encouraging to see a government department making an effort to crack down on invasions of privacy.

More info at: <http://www.abc.net.au/news/newsitems/200608/s1721505.htm>

David Shaw, Senior Software Engineer dshaw@avaya.com

✶ TiVo Is Watching When You Don't Watch, and It Tattles

<Monty Solomon <monty@roscom.com>>

Sun, 20 Aug 2006 04:47:40 -0400

TiVo is starting a research division to sell data about how its 4.4 million users watch commercials - or, more often, skip them: TiVo users spend nearly half of their television time watching programs recorded earlier, and viewers of those recorded shows skip about 70 percent of the commercials.

[Source: Saul Hansell, TiVo Is Watching When You Don't Watch, and It

Tattles, *The New York Times*, 26 Jul 2006; PGN-ed]

<http://www.nytimes.com/2006/07/26/technology/26adco.html?ex=1311566400&en=143cb4893c1c45a9&ei=5090>

✶ The SAFEE Project (was: Anti-hijack Software, Sanders, [RISKS-24.38](#))

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>

Sun, 20 Aug 2006 14:44:06 +0200

Nickee Sanders reports from Yahoo that:

A joint European effort is working on software that would enable remote control of an aircraft that could override any attempts by

hijackers to control the plane, and force a safe landing..... The project is budgeted for 36m Euros.

Please let us try to get this straight. This comment suggests that the EU is putting 36m Euros into developing control SW for commercial aircraft. This is not so, as far as I can tell. The SAFEE project is a *research* project which is focused on the implementation of onboard threat detection systems and the provision of reliable threat information to the flight crew. In the decision making and response management process, secured air/ground exchange of threat level information is foreseen. SAFEE also anticipates the future use of the European Regional Renegade Information Dissemination System (ERRIDS) by all organizations involved in response to acts of unlawful interference on-board aircraft.

(<http://www.safee.reading.ac.uk/about.htm>)

Notice that there is no mention of control SW here, but rather of detection systems and reliable information systems. According to the information brochure which one may download at http://www.safee.reading.ac.uk/SAFEE_brochure.pdf there are five sub-projects. One of the five subprojects is "flight reconfiguration: includes an Emergency Avoidance System (EAS) and a study of an automatic guidance system to control the aircraft for a safe return". Notice the wording: a *study*, not writing control SW.

One of the other subprojects is concerning with secure air-ground communication. About time. Data exchange between aircraft and

ground has
been clear-text-based without effective authentication, and it
is about time
this was changed (I regard authentication as essential).

I see one academic partner in the project (the University of
Reading) and a
lot of commercial partners. Research work by commercial project
partners is
subsidized to a level of 50%, which means that of this 36m
(again note: I
haven't checked this figure), roughly half of it will be paid by
the
participants themselves (the Uni Reading will get 100%).

So the risk highlighted by this note turns out not to be the
reported
one. How to avoid it: check sources before distributing rumors.

Peter B. Ladkin, Causalis Limited and University of Bielefeld
www.causalis.com www.rvs.uni-bielefeld.de

⚡ Re: LA power outages ([RISKS-24.37,38](#))

<Kent Borg <kentborg@borg.org>>
Tue, 22 Aug 2006 15:41:11 -0400

It is **so** hard to do redundancy on an industrial-scale. I.e.,
for a large
data center. One reason the attempt is so frequently doomed is
that is is
SO hard to test a critical system.

Here is a true story of such a failure.

I know of a facility has a diesel generator, and even plenty of
diesel,
enough for easily powering critical systems for a long time.

Wanting to be
safe they test their generator every month.

Time passes. Something goes wrong with the utility power, so
the generator
fires up. All is running as expected--until the generator stops.

Problem: All that diesel. It can't all sit in a gravity-fed
tank on top of
the generator, most of it is in the big tanks, some distance
off, and fed
with a pump.

Specific Problem: The pump was powered off the utility power not
the
generator power; works great during monthly tests, but doesn't
work well at
all when the utility is down.

✶ At least the extension cord worked (Weinstein, [RISKS-24.38](#))

<Mike Albaugh <albaugh@perilin.com>>
Fri, 18 Aug 2006 17:00:31 -0700

Lauren Weinstein pointed out the risks of power-failure to
"bleeding edge"
tech such as VoIP over cable-modem in "Your Cable Company --
powered by the
guy with the extension cord".

Lately AT&T (re-branded SBC) has been running a lot of
advertising making the
same point, and pretty much suggesting that you are putting your
life in
danger by switching away from them.

Maybe yes, and maybe no. I recently had a 36-hour (after I got
home and

reported it) service outage on my POTS (Plain Old Telephone Service), as provided by SBC. Clear weather, No power outage. Several of my neighbors had much the same problem, at about the same time, but SBC denied that the truck they had parked over the neighborhood cable vault had anything to do with it. It had to be in my internal wiring (yeah, unable to cope with "no battery", let alone "no dialtone" at the demarcation point).

RISK: Assuming that the risk a competitor tells you about is the only one that exists. Why any sane person would go for "Triple Play" is beyond me.

Reality: The old "public service" attitude (don't laugh, many PacBell folks did indeed have it) is dead and buried.

⚡ Re: ... Your Dell laptop battery must be OK! (Miller, [RISKS-24.38](#))

<Dave Blake <dave.blake@tiscali.co.uk>>

Mon, 21 Aug 2006 16:25:30 +0100

Dan Miller asks what happens when you do enter (correctly) an ID for a potentially faulty battery into the dellbatteryprogram.com site. The answer is that the site takes you directly to an order page so that you can request a replacement battery. At least there is no "Are you sure that you want to replace your potentially explosive battery" step.

More annoying from my point of view is that I raised a support call with Dell late last month (21 Jul to be precise) as the battery light

on the laptop which was normally green had begun to flash an intermittent red light. After a week or so of emails I was basically fobbed off with a normal-operation-for-a-year-old battery story. I now find that this issue had already been made public in a number of sources, and I find it incredible that Dell has been so slow to react.

<http://www.signonsandiego.com/news/tech/20060712-1221-cargoplanefire.html>

http://www.boingboing.net/2006/07/28/dude_your_dell_just_.html

The BoingBoing story relates how a Dell laptop burst into flames in an office. So far so frightening, but as I work mainly at home and often leave the machine on overnight unattended running AV scans or downloads, in the room next to my daughter's bedroom that I use an office (which of course does not benefit from any of the anti-fire devices that a normal commercial office might have) I find the thought of what might have happened absolutely bloody terrifying.

Then, whilst checking the URLs for this note, I come across the story that the batteries were manufactured by Sony and that they knew of these potential problems 10 months ago. Well, after the music CD rootkit fiasco earlier in the year we all know that Sony seems to have a certain contempt for its customers but I think that this latest story takes the biscuit. There's a whole world of difference between compromising the security of a customer's PC , and potentially killing or maiming someone. Furthermore Sony management could perhaps be forgiven for failing

to grasp the rootkit issue; they can have no such defence over the rather simple issue that their product might burst into flames or explode.

<http://www.macworld.com/news/2006/08/21/battery/index.php>

Lastly, the Macworld story contains the following statement:-

"Fujitsu, Toshiba and Hewlett-Packard (HP) said on Thursday that they use Sony Li-ion batteries with their systems, but that the batteries are different from those being recalled by Dell. The companies said they did not see a fire risk for customers and did not plan on doing a battery recall."

Anyone feel comforted by that?

⚡ Re: ... Your Dell laptop battery must be OK! (Miller, [RISKS-24.38](#))

<Brent Kimberley <brent_kimberley@rogers.com>>
Tue, 22 Aug 2006 21:23:11 -0400 (EDT)

I enjoyed reading Dan Miller's "Your Dell laptop battery must be OK!"

<http://catless.ncl.ac.uk/Risks/24.38.html> .

A new disclaimer has been added to the Dell battery program website:

<https://www.dellbatteryprogram.com/>

Please verify you entered your PPID correctly before submitting
Common errors include distinguishing between alphanumeric characters:

letter "O" from the number "0"

letter "S" from the number "5"
letter "l" from the number "1"

[This disclaimer nibbles off a little of the pain. But the battery model number situation reminds me of license-plate confusions, where similar caveats are presumably issued to police officers. Or, if this ever became connected with a serious law-enforcement case, might we expect Congress to seek legislation that makes certain confusion-causing characters illegal, such as in 00S51I?]

✶ "IT Security Project Management", Susan Snedaker

<Rob Slade <rmslade@shaw.ca>>
Mon, 21 Aug 2006 13:43:45 -0800

BKITSCPM.RVW 20060808

"IT Security Project Management", Susan Snedaker, 2006, 1-59749-076-8,

U\$59.95/C\$77.95

%A Susan Snedaker info@virtualteam.com

%C 800 Hingham Street, Rockland, MA 02370

%D 2006

%E Russ Rogers

%G 1-59749-076-8

%I Syngress Media, Inc.

%O U\$59.95/C\$77.95 781-681-5151 fax: 781-681-3585 www.syngress.com

%O <http://www.amazon.com/exec/obidos/ASIN/1597490768/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/1597490768/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/1597490768/>

[robsladesin03-20](#)

%O Audience i- Tech 1 Writing 1 (see revfaq.htm for explanation)

%P 612 p.

%T "IT Security Project Management"

Chapter one is an introduction, but also something of a preface to the book.

In terms of the intended audience, the author states that it is assumed

readers know the basics of project management and also network security.

The text, therefore, is proposed to be an operational framework for

designing an information technology security project plan.

However, as the

material goes on to describe the components of such a plan only network

items are listed: physical security, applications security, databases,

business continuity, and a host of other considerations are notable by their

absence, and even the vital element of policy is buried as a minor

ingredient. There is a vague and verbose outline of risk and cost/benefit

analysis, and a list of success factors that range from the glaringly

obvious (management support) to the counterproductive (standard off-the-shelf infrastructure is recommended even though this practice is

known to increase the likelihood of attacks).

Chapter two defines security projects, but mostly in terms of the sections

of a proposal. Organizing the project, in chapter three, lists various

project management factors, probably the most significant being the

composition of the team that will define the project. (Didn't we do the

definition in chapter two?) Ensuring quality, in chapter four, seems to

consist of knowing requirements and metrics. Chapter five sees the formation of the project team, which is not the same as the team that defined the project in chapter three. Standard project planning advice is provided in chapter six. Chapter seven is supposed to be about managing the project, but there is little or no mention of the mechanics of management, with the content concentrating on initiation and changes of specifications. The termination phase is reviewed in chapter eight.

Chapter nine, entitled "Corporate IT Security Project Plan," is supposed to be the promised overarching framework. However, after twenty-two pages of legal advice (and two warnings about giving or taking unauthorized legal advice), we find a project outline (missing some of the usual steps) and a haphazard aggregation of project elements, many of which have been covered previously. (Contrary to the recommendation in chapter six, the outline lists a number of items of quite different importance all at the same level.) A random and unstructured collection of security topics makes up the bulk of chapter ten, which is nominally about general IT security planning. The lack of pattern and hodgepodge of subjects seems to confuse even Snedaker: figure 10-1 on page 265 ("Layered Approach to Network Security") and figure 10-5 on page 327 ("Elements of IT Security Requirements") are duplicates. Much the same description is true of IT infrastructure, in chapter eleven, and it also repeats a good deal of the content. Wireless security, in chapter twelve, does have more substance

that is specifically related to wireless technology and risks, although it is strange, given the immediacy of other items in the work (there is a reference to an event that happened on May 24, 2006), that the list of 802.11 protocols does not list 802.11i, which is probably the most secure.

Chapter thirteen, about operations security, does have a bit more organization, but is fairly standard advice about incident response, security awareness, and policy.

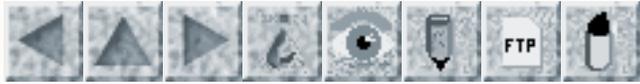
If it is expected that the reader is thoroughly familiar with project management, the primacy and amount of space dedicated to the basic project operations (chapters two to eight, 158 pages) is odd. It turns out that the limiting of the technical content to network areas is of no particular importance, since this volume is really only generic project management advice anyway (and not overly complete, at that). Page 445 notes that "[o]ur goal is not to push you to use outside consultants," but Snedaker is a consultant, and owns a consulting firm. The writing in this book is turgid, the content banal, and the advice incomplete. Given that I am a self-professed professional paranoid, I may perhaps be forgiven for imagining that someone might write a bad book in the hopes that readers, attempting to figure out how to do it themselves, would give up in disgust and look around for someone to make sense of the process for them.

Just a thought.

copyright Robert M. Slade, 2006 BKITSCPM.RVW 20060808
rslade@vcn.bc.ca slade@victoria.tc.ca

rslade@computercrime.org

<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

Search RISKS using [swish-e](#)

Volume 24: Issue 41

Tuesday 5 September 2006

Contents

- [UK 141M-pound benefits computer system shelved](#)
[Martyn Thomas](#)
- [Taxiway altered before KY crash](#)
[PGN](#)
- [The Case of the Patriot System in the Gulf War](#)
[Diego Latella](#)
- [High-tech Product Sabotage](#)
[Peter Mellor](#)
- [British MP falls foul of wiki-d pranksters](#)
[M. Hackett](#)
- [Swedish Atomic Power Plant Shutdown](#)
[Debora Weber-Wulff](#)
- [Another power outage](#)
[Kurt Fredriksson](#)
- [Re: LA power outages](#)
[Michael Bacon](#) [Merlyn Kline](#)
- [Re: Your Cable Company ...](#)
[Robert de Bath](#)

- [More on the Sony lithium-ion laptop battery fire issue](#)
[Curt Sampson](#)
 - [Spread sheets weak point of Security](#)
[Al Macintyre](#)
 - [Re: LA power outages](#)
[Rex Black](#)
 - [Brave New Ballot, Avi Rubin](#)
[PGN](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ UK 141M-pound benefits computer system shelved

<"Martyn Thomas" <martyn@thomas-associates.co.uk>>

Tue, 5 Sep 2006 14:45:13 +0100

"A new computer system used to process benefits payments has been scrapped at a cost to the taxpayer of (UK) 141M pounds, the BBC has learned. The IT project, key to streamlining payments by the UK Department for Work and Pensions (DWP), was quietly axed at an internal meeting last month. ... It is the latest in a long series of computer problems for the government."

[Source: BBC News, 5 Sept 2006]

http://news.bbc.co.uk/1/hi/uk_politics/5315280.stm

[Phillip Hammond, the Conservatives' shadow work and pensions secretary,

is quoted: "It is pretty disgraceful that after two and half years of

spending public money on this project, the government has walked away from

it. We never hear of somebody actually losing their job because they

have failed to implement a project they were responsible for." PGN-ed]

✈ Taxiway altered before KY crash

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

Mon, 28 Aug 2006 16:09:44 PDT

The taxi route for commercial jets at Blue Grass Airport was altered a week before Comair Flight 5191 took the wrong runway and crashed, killing all but one of the 50 people aboard. Both the old and new taxiways to reach the main commercial runway cross over the shorter general aviation runway, where the commuter jet tried to take off on 27 Aug 2006. [Source: Crash Probe Focuses on Use of Shorter Runway, Richard Fausset and Alan C. Miller, *Los Angeles Times*, 28 Aug 2006; PGN-ed; more details in subsequent reports]

<http://www.latimes.com/news/nationworld/nation/la-082806plane,0,242799.story?coll=la-home-headlines>

✈ The Case of the Patriot System in the Gulf War

<Diego Latella <Diego.Latella@isti.cnr.it>>

Mon, 04 Sep 2006 14:18:00 +0200

Diego Latella, The Case of Patriots in the Gulf War. [in italian]
MAGAZINE: SAPERE - Ed. Dedalo srl - www.edizionidedalo.it
Directors: C. Bernardini and F. Lenci

This paper addresses the controversy on the performance of the Patriot

system ATBM during the 1991 Gulf War. The controversy has been initiated by the seminal work of Prof. T.A. Postol and his colleagues at MIT, where several aspects of Patriot performance have been analysed and declarations of Army officials as well as the press have been questioned.

The paper is aimed at the general (although motivated) public more than specialists. It starts by giving a brief introduction to the technical features of the system and its development history. The dramatic scarcity of data concerning the events in the Gulf War is then addressed, and reasons for understanding it are discussed. The most significant failures of the system during the Gulf War are presented, in contrast to the initially overly positive assessments of the success of the system during the war. The discussion is broadened including issues from the debate involving Postol's group, GAO, the Army, Raytheon researchers, and the Panel On Public Affairs of the American Physical Society (which, incidentally, judged very positively the work of the MIT group). Some personal closing remarks are presented on the use of computers in war, having to regret that not so much has changed, since SDI, on the expectations many people, including researchers, still put on computers, despite the lessons we should have learned on their practical as well as conceptual limitations. The paper includes a rich bibliography with more than sixty references.

Dott. Diego Latella, Ist. di Scienza e Tecnologie
dell'Informazione A. Faedo
I56124, Pisa, ITALY +39 0503152982 <http://www.isti.cnr.it/People/>

[D.Latella](#)

[The translation into English is Diego's, although it has been PGN-ed.

Even with my limited ability to read Italian, the original article appears to be very well researched. PGN]

⚡ High-tech Product Sabotage

<Peter Mellor <MellorPeter@aol.com>>

Fri, 25 Aug 2006 20:25:51 EDT

The following is an extract from an article based on the series "Trust me I'm an economist", BBC2. (Second episode 7pm on 25th August 2006.) The author and presenter is Tim Harford, a *Financial Times* columnist and author of "The Undercover Economist".

Supermarkets package their cheapest products to look more like famine relief than something you'd want to pay for. It's not because they can't afford sexy packaging even for their cheapest foods - it's because they want to persuade richer customers to buy something more expensive instead.

Economists call this "product sabotage" and it can reach extreme levels.

In the hi-tech world it is common to produce a high-specification product, sold at a premium price, and then sell the same product more cheaply with some of the functions disabled.

Intel did this with its 486 computer chip in the early 1990s, and IBM did

it with a printer: the economy version for home users was simply the

top-of-the-range model with a chip in it to slow it down.

These tactics might seem sneaky or unethical, and they certainly don't go

down well with customers.

Yet frustrating as it is, product sabotage is often the cheapest way to

produce two different versions of a product. For the hi-tech industry the

alternative is to design the whole product twice.

And two different versions are what you need if you want to reach

price-sensitive customers.

The full article is on:

<http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/business/5274352.stm>

During the 1970s when working for ICL, I was told by customer support

engineers that the 'conversion' of a 1902 mini-mainframe to the faster 1902A

model was to snip one connecting wire on the back-plane. Plus a change ...

Peter Mellor; Mobile: 07914 045072; e-mail: MellorPeter@aol.com

British MP falls foul of wiki-d pranksters

<"M. Hackett" <dist23@juno.com>>

Sat, 2 Sep 2006 01:47:56 -0700

Any fool could tell you that [mixing] Wikis and policy making could only result in this kind of mess.

Currently I am considering the possibility bulk e-mailing UK parliamentarians (or UK PMO / Royal Palace) for an undisclosed client. In my case the matter concerns an international broadcasting linkage between Canada and the UK. So few political wikis exist to get your MP or MLA's attention -- that bulk e-mail and bulk faxing has become the only solid and workable alternative.

Max Power, CEO, Power Broadcasting, <http://HireMe.geek.nz/>
British MP falls foul of wiki-d pranksters

A British Government Minister may have thought he was keeping up with modern trends when he put a draft policy on the Internet on Friday, but he was soon left red-faced when hundreds of pranksters defaced it.

Weblogging, techno-savvy Environment Secretary David Miliband, tipped as a bright young spark in Prime Minister Tony Blair's administration, had put a draft "environment contract" on his department's website, setting out social responsibilities for people, government and businesses.

But embarrassed administrators were forced to haul it down after more than 170 cyber-jokers trashed the document by adding in bizarre paragraphs for fun.

The page used "wiki" editing techniques, which allow readers to alter the content.

A heading of "Who are the parties to the environmental contract?" became,
"Where is the party for the environmental contract? Can I come?
Will there
be cake? Hooray!"

Another asked: "What would an environmental contract for energy look like?
Will it look like my face? My beautiful face?"

The tricky question of "what tools can be used to deliver the environmental contract?" received the answer: "Spade, Organic Yoghurt Stirrer, Old washing up liquid bottle, Sticky Back Plastic."

Meanwhile, a list of tools that "create the right incentive frameworks" was doctored to include "Big stick" and "Owl magnet".

Some of the Internet pranksters put the boot into the Government when monkeying around with the text.

Under a list of things citizens should do, one wag added: "Pay a higher proportion of their income to the government, and see little tangible improvement in their standard of living".

One passage said everyone had the capacity to tackle environmental problems, but that people were too often dissuaded by "doubts about whether our actions will make any difference".

One joker swiftly tagged on: "Besides which we just can't help but meddle, interfere, impose our views on others, and generally use taxpayers' resources in ways that are wasteful except in our own self-aggrandisement".

Word about the document spread like wildfire across several Internet weblogs.

Administrators were forced into action and left a message of their own:

"Please note - the Wiki has been 'locked' for the time being to prevent editing.

"Thanks to everyone for their interest so far - do visit again and continue the discussion. In the meantime, you're welcome to read the comments and materials submitted."

A spokeswoman for the red-faced Department for Environment Food and Rural Affairs said the page was an experiment.

"It's unfortunate that these things do happen. We are currently looking at security on the site," she said.

⚡ Swedish Atomic Power Plant Shutdown

<Debra Weber-Wulff <D.Weber-Wulff@fhtw-berlin.de>>

Sun, 03 Sep 2006 00:22:49 +0200

[This has not been widely reported in the mainstream press, which, given the gravity of what happened shocks me rather more than what happened - dww]

On August 17, 2006, there was a class two incident that occurred at the Swedish atomic reactor Forsmark. A short circuit in the electricity network

caused a problem inside the reactor and it needed to be shut down immediately, using emergency backup electricity. However, in two of the four generators, which run on AC, the AC/DC converters died. They disconnected, leaving the reactor in a state where the operators did not know what the current state of the system was for approx. 20 minutes. A meltdown could have occurred, such as we had in Tschernobyl.

In Sweden, the government immediately shut down all reactors that were built similarly until the problem could be cleared up. In Germany, people were insisting that Brunsbüttel was built similarly, but the company operating the reactor (in both cases, Forsmark and Brunsbüttel: Vattenfall) insisted it was not the same. When it was discovered that Brunsbüttel was indeed the same, the German environmental minister, Sigmar Gabriel, threatened to shut it down right away. But he has been pacified and the reactor is still running.

This seems to be a very similar problem to the LA situation - the emergency systems had not been tested with the grid electricity going off. Additionally, it appears that Brunsbüttel has had three incidents in 2002 pertaining to the emergency electricity system.

According to the taz from August 31, 2006, there exists a list of 260 security problems with Brunsbüttel which the ministry in Kiel is keeping under wraps. The ministry says that a list does exist, but refuses to publish it at the same time it is telling Vattenfall that it is not communicating its problems properly.

The risks involved here are very seldom but very lethal - a core meltdown is no joke.

An extremely technical report can be found here:

<http://www.neimagazine.com/story.asp?sectionCode=132&storyCode=2038313>

Prof. Dr. Debora Weber-Wulff, FHTW Berlin, FB 4, Treskowallee 8, 10313

Berlin GERMANY +49-30-5019-2320 <http://www.f4.fhtw-berlin.de/people/weberwu/>

Another power outage

<"Kurt" <kurt.fredriksson@ieee.org>>

Wed, 30 Aug 2006 15:55:45 +0200

This happened many years ago now, but might be of interest, as an example of an omission of looking at the whole system.

We had a computer center with a large battery backup. The 3-phase AC power was converted to DC, which kept the batteries fully loaded. The power for the servers was converted from DC to 3-phase AC.

One day the latter converter broke, so we only got 2 phases of power.

(There was no interruption in the mains.) We then, to our horror, discovered that there were no switches installed to bypass the faulty converter, and we thus had to close down all servers.

The obvious remedy was to install those switches.

Nobody had thought of the possibility that the converters might fail. Not surprisingly, as these converters are used in million of telephone exchanges all over the world, and had an impressing MTBF.

Kurt Fredriksson

✶ Re: LA power outages ([RISKS-24.37](#),38,39,40)

<Attila The Hun <attilathehun1900@yahoo.co.uk>>

Wed, 30 Aug 2006 02:02:03 -0700 (PDT)

A data centre in London, UK suffered a total power outage on Sunday, 23 Jul 2006 when the incoming supply and the in-house stand-by generation failed. Other events contributed to a loss of service lasting 11 hours and four minutes.

The events ran as follows:

At 10:56 a public supply 132kV to 11kV transformer failed with consequential failure in the 40kV to 132kV transformer feeding the area of London that feeds the data centre. Incoming power failed on all six cables.

Generators 1 and 3 started OK, but generator 2 did not -- owing to insufficient air pressure to engage the starter motors. A stand-by diesel-powered air-compressor was tried, but could not maintain pressure in the air-starter piping.

Generator 1 began to overheat and shut down and generator 3 shut down shortly afterwards due to a high load condition.

While the generators were running, the supply was repeatedly in and out of tolerance. When out of tolerance, the UPS batteries provided the primary power source and this drained the power from the batteries even when the generators were running.

As a result and just before generators 1 and 3 failed, UPS3 shutdown safely and went into bypass mode. No fuses were blown.

When the generated power were finally lost, UPS3 reverted to a non-bypass configuration. The remaining UPSs then went into normal battery back-up and carried the load for 22 minutes at which time the UPS modules began to discharge their batteries.

UPS1 then shut down on a "battery low" alarm for one module. When the second module reached "battery low", there was no power available on the module and it shut down without going into bypass. This cascaded until the last module was taking the entire load and, as this discharged, the voltage and frequency dropped resulting in the inverter thyristors failing to switch off. This caused both inverter and battery fuses to blow as well as one of the inverter thyristors themselves.

UPS 2 exhibited a similar failure.

All UPSs were then off and auto bypass was not enabled.

When the mains were restored, raw mains was not provided

directly to the PDUs. As a consequence, the input breaker shunt-tripped. This could not be reset until the UPS power has been restored at the PDU level and then each input breaker had to be manually re-set.

While this was going on, Building Management System (BMS) connectivity was lost and the fire alarm went off. The Fire Brigade arrived and evacuated the building.

An hour later, the Fire Brigade had confirmed the safety of the building, the fire alarm system had been taken off-line and staff had re-entered the building

Commercial power was restored at 13:42.

All DC and HVAC systems normalised without intervention, but the UPS systems had to be restored manually.

About one hour after this, UPSs 1 and 3 were brought back online.

A further hour later UPS 2 was brought back online.

Half an hour later, data centre personnel began to restore various UPS PDUs to operation.

Some 90 minutes after this, UPS power was briefly restored to the BMS and the Integrated Management and Monitoring System (IMMS) began to report sporadic alarms.

By 20:00 all UPSs were back online.

Two hours later, service had been restored, albeit that some customers were

suffering odd failures the following day - possibly owing to the loss of power to equipment that had been previously running continuously for thousands of hours.

Some years before, an international bank in London suffered a power outage while having its UPS serviced.

They had two levels of battery UPS with stand-by generation through diesel-powered alternators. Level One UPS was scheduled for maintenance.

It was taken down and (Sod's Law at work!) within minutes the incoming supply failed (as a result of "JCB-fade"). "Never mind!" the engineers cried, "There is always the Level Two UPS". Sadly, this did not take up the load, owing to the previously undetected failure of an "AND" circuit that noted the absence of incoming mains power and a low voltage condition on UPS1. "Never mind!" the engineers cried again. "The stand-by generators will start and carry the load." They didn't! The reason? The stand-by generators required a signal from UPS1 ... which was down for maintenance.

Attempts to manually start the SBGs failed, firstly because the batteries were flat (!) and secondly (after replacing the batteries) because the manual-start process still required a signal from UPS1 to release an interlock. Some five hours of blackout was experienced before the incoming supply was restored.

Michael "Streaky" Bacon

✉ **Re: LA power outages (Fairfax, [RISKS-24.40](#))**

<"Merlyn Kline" <merlyn@zynet.net>>

Wed, 30 Aug 2006 10:30:02 +0100

[...]

> Redundancy isn't hard. Engineering is hard.

But not impossible. Stephen Fairfax was able to think of a wide range of possibly untested failure modes for this system while dashing off an email.

If suitably paid, I've no doubt he (and many others) could think of a

comprehensive, even exhaustive, list and design and implement a suitable

test programme. But who would be willing to pay? The results of losing a

data centre rarely compare to the results of losing a Boeing or a skyscraper

or a power plant. Of course occasionally they do. I wonder how well tested

those data centres are?

Merlyn Kline

✉ **Re: Your Cable Company ... ([RISKS-24.37](#))**

<Robert de Bath <robert\$@debath.co.uk>>

Wed, 30 Aug 2006 07:04:24 +0100 (BST)

On Sat, 12 Aug 2006, Lauren Weinstein wrote:

> I found it rather amusing, in a "sad commentary" sort of way.

I disagree with the "sad commentary" part of this, to explain.

A UPS is for risk management not risk elimination you decide two numbers

(a) How long do you expect to need internal power.

(b) How long does it take to do a controlled shutdown.

Add them together, add some more for growth and luck. The numbers you come up with then reduce the risk to an "acceptable" level.

But there's a twist to the first number. For example in a hospital computer system you only need batteries for long enough to get the diesel generator started. You only need enough diesel to keep you going until you are sure you can get a refill. Exactly the same reasoning has happened with that telecom node. (possibly after the fact of course)

Robert de Bath <robert\$ @ debath.co.uk> <<http://www.debath.co.uk/>>
>

More on the Sony lithium-ion laptop battery fire issue

<Curt Sampson <cjs@cynic.net>>

Wed, 6 Sep 2006 00:18:01 +0900 (JST)

Here's a link to an interesting analysis that's rather more extensive than others I've seen, perhaps in part because it relies on subscription-only sources to Japanese news sites:

http://japaninc.typepad.com/terries_take/2006/08/index.html#top

The particularly good bit:

The technical causes of the batteries overheating were well explained in a recent Nikkei interview of a professor at Kyoto University, who is an expert on battery technology. He points out that there are two possible, complementary reasons for the Dell notebook fires -- one of which offsets some of the blame from Sony.

Firstly, there was the well publicized manufacturing failure, consisting of metal particles that were introduced into the battery electrolyte and which can eventually lead to internal short circuits and thus overheating. Sony takes full responsibility for this.

The second reason, however, is probably not so well known, but allows Sony to share the blame with with Dell and Apple.

Apparently some PC designs by both companies push the Lithium-ion battery technology past its safe point by virtue of the fast recharging cycle the makers have implemented. According to the professor, when Lithium cells are exposed to rapid charging, they can form metal fragments through chemical reaction between the electrodes and a high concentration of Lithium atoms.

Once formed, these conductive metallic fragments can penetrate the plastic separator between the positive and negative electrodes, causing major short-circuits and thus catastrophic over-heating. This failure in circuit design is probably why Sony investors are betting that

the company

won't have to cover the entire cost of the recall.

Curt Sampson <cjs@cynic.net> +81 90 7737 2974

⚡ Spread sheets weak point of Security

<Al Mac <macwheel99@sige.com.net>>

Sun, 03 Sep 2006 15:53:39 -0500

Computerworld rediscovers that it is well known in business, that the official data may be well secured in data bases, with sensitive data going to trusted employees who reorganize the data in spread sheets BI tools that are not as well secured against data breaches.

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9002950&source=rss_topic17

Story found thanks to <http://socrates.berkeley.edu:7077/it-security/>

⚡ Re: LA power outages (Borg, [RISKS-24.40](#))

<Rex Black <rexblack@ix.netcom.com>>

Fri, 25 Aug 2006 22:18:09 -0500

Finding and fixing this particular defect actually comes at almost zero cost. Here's what happens:

1. Professional tester designs high-fidelity test, including a

step that

involves powering down of the fuel pump.

2. During a test case review with the system engineers, someone says, "Hey,

we can't do that, if the diesel engine is run dry, it'll break."

3. Professional tester says, "Yes, okay, but let's just suppose we *did* run

the test. Guess what I learned while designing the test? The fuel pump

is connected to utility power with no fail-over to generator power. So,

when utility power fails, the pump stops, which means the diesel soon is

running without fuel, which means that not only does the diesel engine

become damaged, but we don't get our backup power."

4. System engineers say, "Ohhhhh." System engineers leave test case review,

go off and solve problem.

5. Professional tester, without running a single test, saves the organization thousands, potentially millions of dollars.

I have seen scenarios like this happen dozens of times in my career being a

professional tester and managing professional testers. Amateur testers--i.e., people who do not make a study and profession of the field of

testing--will usually miss situations like this.

Now, I will grant you that there are plenty of instances where a truly

high-fidelity test *is* judged by management to be cost-prohibitive. For

example, some people do not performance test in completely accurate test

environments, which casts a lot of doubt on their performance test results.

(By the way, please note that we are talking about *software*

testing here,
so this is a case where the combinatorial explosion is not
actually what
gets you into trouble; in fact, the combinatorial explosion is
not that
difficult to deal with.) The explanation is usually, "It'll
cost too much
to replicate the production environment." Of course, that was
exactly the
reason why NASA didn't test the effect of foam strikes on
shuttle wings,
which were going on for years before the US lost one very
expensive shuttle
and seven very expensive--indeed, to their families, priceless--
astronauts.
I bet that foam strike test that was proposed to be run at
Southwest Texas
Research Institute--and cancelled due to cost considerations--
looks like a
bargain to those same NASA managers now....

Rex Black Consulting Services, Inc. 31520 Beck Road, Bulverde,
TX 78163 USA
CTO, Pure Testing, Pvt Ltd +1 (830) 438-4830 www.
rexblackconsulting.com

Brave New Ballot, Avi Rubin

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

Mon, 28 Aug 2006 16:09:44 PDT

Brave New Ballot:

The Battle to Safeguard Democracy in the Age of Electronic Voting

Aviel D. Rubin

Morgan Road Books (Doubleday/Random House)

\$24.95 ISBN 0-7679-2210-7

Avi Rubin performs a true patriotic duty with this book. He
shows that

without voter-verified records, votes can be lost, election outcomes can come into doubt, and public cynicism in the political process surely grows. *Brave New Ballot* is an interesting story of a talented computer scientist who found himself in an adventure because of his dogged effort to make America's voting technology consistent with her democracy.

U.S. Representative Rush Holt (D-NJ)

This book is a very readable introduction to the ongoing challenges. Although it is written as a rather personal narrative in a largely nontechnical manner, it captures many of the important issues underlying the need for and general lack of integrity of the election process.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 42

Weds 13 September 2006

Contents

- [Risks of exhaustive testing](#)
[Jim Horning](#)
 - [Tax blunder undermines Belgian federal budget](#)
[Wim Heirman](#)
 - [New UK biometric passports & identity theft](#)
[C Greenock](#)
 - [Avi Rubin's latest report as an election judge](#)
[PGN](#)
 - [Princeton's Diebold analysis](#)
[Feldman-Halderman-Felten via PGN](#)
 - [REVIEW: "Scene of the Cybercrime: Computer Forensics Handbook", Shinder](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Risks of exhaustive testing

<"Horning, Jim" <Jim.Horning@sparta.com>>

Tue, 12 Sep 2006 17:58:45 -0700

After 45 years, I've finally gotten round to documenting the story of a small subroutine whose QA included running 10,000,000 distinct test cases. Since the background is rather complicated and non-linear, I've done it via a collection of web pages, rather than try to put it all in one email message.

<http://horningtales.blogspot.com/2006/09/exhaustive-testing.html>

"The most exhaustively-tested program that I know of still had a serious bug when it was released... If you have ten million test cases, you probably missed one."

✶ Tax blunder undermines Belgian federal budget

<Wim Heirman <wim.heirman@ugent.be>>

Wed, 13 Sep 2006 13:59:27 +0200

"The Belgian federal budget for 2006 will need to be reviewed after the tax administration discovered a "calculation error" of 883M Euro. ... In total, errors in the processing of 26 tax reports led to an overestimate of federal income by 883.6M. One taxpayer was told he would be refunded 99.9M, another one would have to pay 187.9M extra. ... Most of the errors were made between 9 and 22 May. For an unknown reason, several safety filters in

the tax calculation software were disabled at that time. Manual checks did not reveal the error."

And further down the article, a quote from a high-ranking officer of the tax administration dated end February:

"The software contains a number of automatic filters to discover irregularities in the tax reports. ... But to speed things up, we have now strongly simplified these filters."

A not so nice surprise for our ministers, just weeks before the (local) elections. And a cold shower after a summer of handing out budgetary presents in the expectation of a 500M rise in tax income since last year...

[Source: De Standaard, 13 Sept. 2006]

<http://www.standaard.be/Artikel/Detail.aspx?artikelId=GA111JA8J>
and
<http://www.standaard.be/Artikel/Detail.aspx?artikelId=G8H11J3MC>
(in Dutch)]

ir. Wim Heirman, ELIS Department, Ghent University, Belgium +32-9-264.95.27
E-mail: wim.heirman@elis.UGent.be <http://www.elis.UGent.be/~wheirman/>

🚩 New UK biometric passports & identity theft

<C Greenock <cigwork@yahoo.co.uk>>
Fri, 8 Sep 2006 15:53:49 +0100 (BST)

It was noted recently by one of the 'new totalitarian'

enthusiasts for the new passport that it shouldn't be possible to interrogate the new UK 'biometric' passport at any other than a distance of a foot or two.

It was then pointed out (on RISKS) that read range can be extended with a sufficiently powerful transmitter/reader. However it seems that the way in which passports are delivered means that a standard reader is all that is required to read the new passport and still be able to steal the information it contains.

I recently renewed my passport as part of the protest about the introduction of the 'ID card'. I received it through the post. It was delivered by a courier company (not Royal Mail). Despite there being nothing blatantly obvious on the envelope to identify it as a passport the delivery driver knew that it was a passport. If this is the case then it seems to me that it would be fairly straightforward for a courier using a standard RFID reader to scan each passport, in its envelope, as he or she delivers it and hand the details on to an accomplice at some later time. We know that the encryption has already been broken.

So. No need to steal the passport, no need even to open the envelope containing the passport. All the details taken & no evidence to show it.

One other thing that amused and irritated me. According to the leaflet that came with the passport the chip and aerial are fragile and I should

therefore take great care of the passport and not subject it to heat nor magnetic and electric fields (I'm paraphrasing). You have to question the sense of sending out something so vulnerable that it can't withstand the sort of mistreatment that the old fashioned paper document could withstand for years on end.

However the leaflet went on to assure me that the passport reached me, 'in perfect working order'. So that's alright then.

✶ Avi Rubin's latest report as an election judge

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

Wed, 13 Sep 2006 10:27:43 PDT

[This is from Avi Rubin's blog, on his latest experiences as an election judge. This is a extremely relevant item for RISKS. PGN]

My day at the polls - Maryland primary '06

<http://avi-rubin.blogspot.com/2006/09/my-day-at-polls-maryland-primary-06.html>

I don't know where to start. This primary today is the third election that I have worked as an election judge. The last two elections <<http://avirubin.com/judge.html>> were in 2004, and I was in a small precinct in Timonium, MD. This time, I was in my home precinct about 1/2 a mile from my house. We had 12 machines, over 1,000 voters and 16 judges. I woke up at 5:30 in the morning and was at the precinct before 6:00. It is now 10:18 pm,

and I just got home a few minutes ago. As I have made it my custom, I sat down right away to write about my experience while everything was still fresh. In anticipation of this, I took some careful notes throughout the day.

The biggest change over the 2004 election was the introduction of electronic poll books that we used to check in voters. I was introduced to these in election judge training a few weeks ago. These are basically little touchscreen computers that are connected to an Ethernet hub. They each contain a full database of the registered voters in the county, and information about whether or not each voter has already voted, in addition to all of the voter registration information. The system is designed so that the machines constantly sync with each other so that if a voter signs in on one of them and then goes to another one, that voter will already be flagged as having voted. That was the theory anyway. These poll books turned out to be a disaster, but more on that later.

Around 7:15, when we had been open for business for 15 minutes already, a gentlemen shows up saying that he is a judge from another precinct nearby and that they did not receive any smartcards, so that they could not operate their election. We had 60 smartcards, and the chief judge suggested that we give them 20 so that they could at least get their election started. As she was handing them over, I suggested that we had to somehow verify his claim. After all, anyone could walk in off the street and claim

this guy's story, and we would give them 20 access cards. The chief judge agreed with me. The guy pulled out his driver's license to prove who he was, but I told him that we were not doubting who he was, we just wanted to verify that we should give him the cards. He seemed to understand that. After calling the board of elections, we were told to give him the cards and we did. A little later, several voters who came in informed us that news reports were saying that in Montgomery county, there was a widespread problem of missing smartcards. I could only imagine what a nightmare that was for those poll workers because as it was, our precinct did not have this problem, and as you'll see, it was still tough going.

My precinct uses Diebold AccuVote TS, the same one that we analyzed in our study <<http://avirubin.com/vote/analysis/index.html>> 3 years ago. The first problem we encountered was that two of the voting machine's security tag numbers did not match our records. After a call to the board of elections, we were told to set those aside and not use them. So, we were down to 10. We set up those machines in a daisy chain fashion, as described in the judge manual, and as we learned in our training. We plugged the first one into the wall and taped the wire to the floor with electric tape so nobody would trip over it. About two hours into the voting, I noticed that the little power readout on the machines was red, and I thought that this meant that the machines were on battery power. I pointed this out to one of the

chief judges, but she said this was normal. An hour later, I checked again, and this time, the machines were on extremely low power. This time, I took the plug out to of the wall and tried another outlet nearby. The power icon turned green. I showed several of the judges, and we confirmed that the original outlet was indeed dead. Had I not checked this twice, those machines would have died in the middle of the election, most likely in the middle of people voting. I hate to think about how we would have handled that. A couple of hours later, the board of elections informed us that we should use the two voting machines with the mismatched tags, so we added them and used them the rest of the day (!).

When we were setting up the electronic poll books, I took over because I was more comfortable with the technology, and the others quickly deferred to me. So, a couple of hours into the election, when one of the poll books seemed to be out of sync with the others, the judges came and brought me to have a look. It appeared that this poll book was not getting synced with the others. I tested it by waiting for someone to sign in with a different poll book, and then a few minutes later trying to sign in that voter on the one in question. The voter was shown as having not voted yet. I repeated this test for about 20 minutes, but it never registered that voter as having voted, and the poll book was falling behind - about 30 by then - the other poll book machines. I suggested rebooting that machine, and we tried that, but it did not change anything. I pointed out to the chief

judges who were huddled around me as I experimented, that as time went by, this poll book was going to fall further and further behind the others, and that if someone signed in on the others, they would be able sign in again on this one and vote again. After a call to the board of elections, we decided to take this one out of commission. This was very unfortunate, because our waiting lines were starting to get very long, and the check-in was the bottleneck. The last few hours of the day, we had a 45 minute to an hour wait, and we had enough machines in service to handle the load, but it was taking people too long to sign in.

The electronic poll books presented an even bigger problem, however. Every so often, about once every 15-25 minutes, after a voter signed in, and while that voter's smartcard was being programmed with the ballot, the poll book would suddenly crash and reboot. Unfortunately, the smartcard would not be programmed at the end of this, so the poll worker would have to try again. However, the second time, the machine said that the voter had already voted. The first few times this happened, we had some very irate voters, and we had to call over the chief judge. Soon, however, we realized what was happening, and as soon as the poll book crashed, we warned the voter that it would come up saying that they had already voted, but that we knew they hadn't. Then, the chief judge would have to come over, enter a password, and authorize that person to vote anyway. Then we had to make a log entry of the

event and quarantine the offending smartcard. Unfortunately, the poll books take about 3 minutes to reboot, and the chief judges are very scarce resources, so this caused further delays and caused the long line we had for most of the afternoon and evening while many of the machines were idle. Another problem was that the poll book would not subtract a voter from its total count when this happened, so every time we had an incident, the poll book voter count was further off the mark. We had to keep track of this by hand, so we could reconcile it at the end of the day.

At times, the remaining two poll books were way out of synch, but after a while, they caught up with each other. When the lines got really long, we considered the idea of trying to use the third one that had caused problems, but we all agreed that we would feel very stupid if all of them started crashing more. I was worried that synching three of these on an Ethernet hub was more complex than 2, and in fact, they were crashing a bit less often when we had only 2. The whole time I was worried about what we would do if these thing really died or crashed so badly and so often that we couldn't really use them. We had no backup voter cards, so the best we could have done would have been to start letting everybody vote by provisional ballots. However, we had two small pads of those ballots, and we would have run out quickly. I can't imagine basing the success of an election on something so fragile as these terrible, buggy machines.

Throughout the early part of the day, there was a Diebold representative at

our precinct. When I was setting up the poll books, he came over to "help", and I ended up explaining to him why I had to hook the ethernet cables into a hub instead of directly into all the machines (not to mention the fact that there were not enough ports on the machines to do it that way). The next few times we had problems, the judges would call him over, and then he called me over to help. After a while, I asked him how long he had been working for Diebold because he didn't seem to know anything about the equipment, and he said, "one day." I said, "You mean they hired you yesterday?" And he replied, "yes, I had 6 hours of training yesterday. It was 80 people and 2 instructors, and none of us really knew what was going on." I asked him how this was possible, and he replied, "I shouldn't be telling you this, but it's all money. They are too cheap to do this right. They should have a real tech person in each precinct, but that costs too much, so they go out and hire a bunch of contractors the day before the election, and they think that they can train us, but it's too compressed." Around 4 pm, he came and told me that he wasn't doing any good there, and that he was too frustrated, and that he was going home. We didn't see him again.

I haven't written at all about the AccuVote machines. I guess I've made my opinions about that known in the past, and my new book <<http://bravenewballot.org>> deals primarily with them. Nothing happened today to change my opinion about the security of these systems, but I did

have some eye opening experiences about the weaknesses of some of the physical security measures that are touted as providing the missing security. For example, I carefully studied the tamper tape that is used to guard the memory cards. In light of Hursti's report <<http://www.blackboxvoting.org/BBVtsxstudy.pdf>>, the security of the memory cards is critical. Well, I am 100% convinced that if the tamper tape had been peeled off and put back on, nobody except a very well trained professional would notice it. The tamper tape has a tiny version of the word "void" appear inside it after it has been removed and replaced, but it is very subtle. In fact, a couple of times, due to issues we had with the machines, the chief judge removed the tamper tape and then put it back. One time, it was to reboot a machine that was hanging when a voter was trying to vote. I looked at the tamper tape that was replaced and couldn't tell the difference, and then it occurred to me that instead of rebooting, someone could mess with the memory card and replace the tape, and we wouldn't have noticed. I asked if I could play with the tamper tape a bit, and they let me handle it. I believe I can now, with great effort and concentration, tell the difference between one that has been peeled off and one that has not. But, I did not see the judges using that kind of care every time they opened and closed them. As far as I'm concerned, the tamper tape does very little in the way of actual security, and that will be the case as long as it is used by lay poll workers, as opposed to CIA agents.

As we were computing the final tallies towards the end of the evening, one of the Diebold machines froze. We had not yet printed the report that is used to post the results. One of the judges went to call the board of elections. She said she was transferred and then disconnected. We decided to do a hard reboot of it after we closed down the other machines. When we finished the other machines, we noticed that the problem one had somehow recovered, and we were able to finish. Strange because it was frozen for about 10 minutes.

So, this day at the polls was different from my two experiences in 2004 <<http://avirubin.com/judge.html>>. I felt more like an experienced veteran than a wide eyed newbie. The novelty that I felt in 2002 was gone, and I felt seasoned. Even the chief judges often came to me asking advice on how to handle various crises that arose. Several other suggested that I should apply to be a chief judge in the next election cycle, and I will probably do that. The least pleasant part of the day was a nagging concern that something would go terribly wrong, and that we would have no way to recover. I believe that fully electronic systems, such as the precinct we had today, are too fragile. The smallest thing can lead to a disaster. We had a long line of "customers" who were mostly patient, but somewhat irritated, and I felt like we were not always in a position to offer them decent customer service. When our poll books crashed, and the lines grew, I had a sense of dread that we might end up finishing the day

without a completed election. As an election judge I put aside my personal beliefs that these machines are easy to rig in an undetectable way, and become more worried that the election process would completely fail. I don't think it would have taken much for that to have happened.

One other thing struck me. In 2004, most voters seemed happy with the machines. This time around, many of them complained about a lack of a paper trail. Some of them clearly knew who I was and my position on this, but others clearly did not. I did not hear one voter say they were happy with the machines, and a dozen or so expressed strong feelings against them.

I am way too tired now (it's past 11 pm) to write any kind of philosophical ending to this already too long blog entry. I hope that we got it right in my precinct, but I know that there is no way to know for sure. We cannot do recounts. Finally, I have to say a few words about my fellow poll workers. We all worked from 6 a.m. to past 10 p.m. These volunteers were cheerful, pleasant, and diligent. They were there to serve the public, and they acted like it. I greatly admire them, and while the election technology selection and testing processes in this country make me sick, I take great hope and inspiration from a day in the trenches with these people.

[See Avi's blog for some very relevant responses as well. PGN]

Princeton's Diebold analysis

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

Wed, 13 Sep 2006 9:22:18 PDT

Security Analysis of the Diebold AccuVote-TS Voting Machine
Ariel J. Feldman <<http://www.cs.princeton.edu/~ajfeldma>>,
J. Alex Halderman <<http://www.cs.princeton.edu/~jhalderm>>,
and Edward W. Felten <<http://www.cs.princeton.edu/~felten>>

Abstract. This paper presents a fully independent security study of a Diebold AccuVote-TS voting machine, including its hardware and software. We obtained the machine from a private party. Analysis of the machine, in light of real election procedures, shows that it is vulnerable to extremely serious attacks. For example, an attacker who gets physical access to a machine or its removable memory card for as little as one minute could install malicious code; malicious code on a machine could steal votes undetectably, modifying all records, logs, and counters to be consistent with the fraudulent vote count it creates. An attacker could also create malicious code that spreads automatically and silently from machine to machine during normal election a voting-machine virus. We have constructed working demonstrations of these attacks in our lab. Mitigating these threats will require changes to the voting machine's hardware and software and the adoption of more rigorous election procedures.

[See <http://itpolicy.princeton.edu/voting/> for the full paper, executive summary, FAQ, and other studies. PGN]

REVIEW: "Scene of the Cybercrime: Computer Forensics Handbook",

<Rob Slade <rmslade@shaw.ca>>

Mon, 04 Sep 2006 11:38:55 -0800

Debra Littlejohn Shinder

BKSOC CFH.RVW 20060809

"Scene of the Cybercrime: Computer Forensics Handbook", Debra Littlejohn Shinder, 2002, 1-931836-65-5, U\$59.95/C\$92.95

%A Debra Littlejohn Shinder debshinder@sceneofthecybercrime.com

%C 800 Hingham Street, Rockland, MA 02370

%D 2002

%E Ed Tittel

%G 1-931836-65-5

%I Syngress Media, Inc.

%O U\$59.95/C\$92.95 781-681-5151 fax: 781-681-3585 amy@syngress.com

%O <http://www.amazon.com/exec/obidos/ASIN/1931836655/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/1931836655/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/1931836655/robsladesin03-20>

%O Audience n+ Tech 2 Writing 3 (see revfaq.htm for explanation)

%P 718 p.

%T "Scene of the Cybercrime: Computer Forensics Handbook"

There are some good forensics books out there, but there are also a number of forensics titles that are nothing more than pamphlets suggesting that the reader get a copy of EnCase and fool around. Then there is this work. I'm not sure how I got a review book that is four years old, an

eternity in the technical realm, and particularly in security. Astoundingly, Shinder produced a work that cut to the heart of the necessary concepts, without piling on technical trivia that would rapidly go out of date. This volume is as relevant and valuable today as it was when it came out.

The foreword notes that the author, herself from both a law enforcement and a technical background, found that most technical security people know little about law and legal procedures, and that law enforcement personnel know next to nothing about computer internals. She set herself to provide geek info to the cops and cop smarts to the geeks, and to compile a reference to other resources.

She has produced an admirably valuable text.

Chapter one starts out with a bit of a slip, stating that cybercrime is a subcategory of computer crime, but then explains it in such a way as to be basically identical. However, Shinder goes on to provide an excellent review of the problems in defining and categorizing cybercrime, jurisdictional issues, and the difficulties in building a team and infrastructure to fight cybercrime. A concise history of computer crime events and issues, and a review of common dangers, makes up chapter two.

(The material on high-speed Internet is somewhat dated, but the rest is excellent.) In other hands, chapter three's examination of the people involved in cybercrime would be a rehash of old "hacker" stereotypes.

Instead, Shinder gives us criminal psychology, profiling (and

counterexamples to the stereotypes), victimology, and the characteristics of a good investigator.

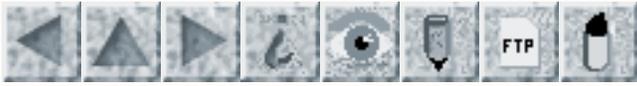
Chapter four looks into computer hardware basics. Techies will think it simplistic, but the content is pitched just right for computer neophytes who need the fundamental concepts and enough detail to step up to further studies. Some may think that the coverage of networking, in chapter five, spends too much time on analogue signaling and old LAN protocols, but you have to remember that digital forensic investigators are not called upon to use standard environments, but to assess the material found in arbitrary ones. The presentation of network intrusions and attacks, in chapter six, has clear representation of the concepts, without deluging the reader with quickly datable minutia.

Chapter seven, turning to cybercrime prevention, presents general information security concepts, with a concentration on networks and cryptography. (As with many, Shinder seems to be fascinated with steganography out of all proportion to its importance.) Implementing system security, in chapter eight, is similar, but with greater emphasis on specific settings. (Although this is very helpful, particularly to the home user, it has limited application to forensics.) Chapter nine looks at cybercrime detection techniques, primarily audit information in its various forms. The collection and preservation of digital evidence is an important and difficult task. Chapter ten does not go into the same level of detail as Michael A. Caloyannides' "Computer Forensics and Privacy"

(cf. BKCMFRPR.RVW), "Computer and Intrusion Forensics" by Mohay et al
(cf. BKCMINFO.RVW), Kruse and Heiser's classic "Computer Forensics"
(cf. BKCMFPRN.RVW), the somewhat challenging "Forensic Discovery" by Farmer and Venema (cf. BKFORDIS.RVW), and Brian Carrier's resourceful "File System Forensic Analysis" (cf. BKFSFRAN.RVW), but presents a broad overview, and has good advice on evidence management and a useful list of resources. Legal systems, types of laws, jurisdictional issues, and the preparation of a case is covered in chapter eleven, which extends "A Guide to Forensic Testimony" by Smith and Bace (cf. BKGDFOTS.RVW).

For anyone just becoming involved in digital forensics, the book is an excellent introduction and overview of the field in its proper context. For those already involved, this manual is both a solid reminder of what needs to be taught to those becoming involved in computer forensics, and also a resource for a number of areas that the individual specialist may not cover every day. Despite the age of the work, in this fast changing environment, Shinder has produced a text of classic depth and lasting value. (Hopefully Syngress will get her to produce updates on a regular basis.)

copyright Robert M. Slade, 2006 BKSOCFFH.RVW 20060809
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<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

Search RISKS using [swish-e](#)

Volume 24: Issue 43

Thurs 21 September 2006

Contents

- [Air Traffic Controllers Chafe at Plan to Cut Staff](#)
[PGN](#)
- [Should you wear a helmet while bicycling?](#)
[Jerry Leichter](#)
- [Cost of online banking typo put on consumer](#)
[Kjetil Torgrim Homme](#)
- [Risks of reprogrammable ATMs](#)
[Mark Brader](#)
- [Segway software gives hard landing](#)
[PGN](#)
- [Yet Another Power Outage](#)
[Mike Swaim](#)
- [Careful with that Fedex account number](#)
[Matt Wilbur](#)
- [Hotel minibar keys open Diebold voting machines](#)
[Ed Felten via PGN](#)
- [Cuyahoga County Primary Election Report](#)
[David Lesher](#)

- [Re: Avi Rubin's latest report as an election judge](#)
[Kurt Fredriksson](#)
 - [SSN-as-ID under scrutiny - again](#)
[Peter B. Ladkin](#)
 - [New way to break into cars](#)
[Gerrit Muller](#)
 - [Thieves sabotage telecom infrastructure](#)
[Gerrit Muller](#)
 - [Cops say teen concocted radio calls](#)
[S Hutto](#)
 - [Regarding High-tech Product Sabotage](#)
[Phil Singer](#)
 - [REVIEW: "Computer Security Basics", Lehtinen/Russell/Gangemi](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈ Air Traffic Controllers Chafe at Plan to Cut Staff

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

Wed, 20 Sep 2006 11:18:07 PDT

A drive by the Federal Aviation Administration to cut the number of air traffic controllers nationally by 10 percent below negotiated levels, and even more sharply at places like the busy radar center here, is producing tension, anger and occasional shows of defiance among controllers. One of the new changes may have safety implications: ending of contractual protection against being kept working on a controller's radar screen for more than two hours without a break. Having just one controller on duty is also problematic [as noted in the recent wrong-runway episode in Lexington

KY ([RISKS-24.41](#))]. [Source: Matthew L. Wald, *The New York Times*, 20 Sep 2006; PGN-ed, TNX to Lauren Weinstein]
<http://www.nytimes.com/2006/09/20/washington/20control.html>

✦ Should you wear a helmet while bicycling?

<Jerry Leichter <jerroldleichter@mac.com>>

Sat, 16 Sep 2006 19:35:18 -0400

We've had previous discussion in RISKS of the unexpected side-effects that can result when human beings respond to safety measures by changing their behavior, taking on risks that previously were too great to feel acceptable.

http://www.eurekalert.org/pub_releases/2006-09/uob-wah091106.php

is a news

release about some research in this area. Dr. Ian Walker spend a great deal of time bicycling around the UK on a bicycle with equipment that measured

how close drivers of different kinds of vehicles came to him when passing.

Half the time, he wore a helmet; half the time, he didn't.

Result: Drivers

approached closer (and average of 8.5 cm) when he was wearing a helmet.

Walker's hypothesis is that drivers see bicyclists wearing helmets as more experienced and competent, hence not in need of consideration.

In other interesting results, when Walker wore a wig so that he looked like

a woman, he was given significantly more room. He also confirmed a feeling

all bicyclist have: Yes, indeed, trucks and buses do approach bicycles more closely (average of 19 cm for trucks and 23 cm for buses) than cars do.

As Walker points out, helmets definitely do protect a rider in low-speed falls. How much they help in collisions with vehicles is harder to say - and if wearing a helmet makes a collision more likely, the net effect is difficult to predict. (Walker was hit twice, once by a bus and once by a truck, during his experiments. He was wearing a helmet both times.)

[Spelling correction in archive copy.]

✶ Cost of online banking typo put on consumer

<Kjetil Torgrim Homme <kjetilho@ifi.uio.no>>

Tue, 19 Sep 2006 10:25:40 +0200

Grete Fossbakk wanted to transfer NOK 500,000 (USD 76400) to her daughter using her online bank account, but entered a digit too many in the account number field. The bank software stripped it silently and transferred the money to a third party. Unfortunately, the recipient immediately withdrew the bounty and started to gamble it away. Meanwhile, the daughter was on vacation, so the mishap wasn't discovered until three weeks had passed. The matter was reported to the police, and they were able to reclaim NOK 100,000 in cash in the man's apartment. Ms Fossbakk has launched a civil claim

against the man for the remainder of the money, but since he lives off social security, the chances of getting it back are slim.

The bank, Sparebank1 Nord-Norge, claims that if you type the wrong number, you have to bear the consequences yourself. The Norwegian bank industry's board of complaints (Bankklagenemnda) will hopefully decide in the case in time for Christmas. The Minister for Consumer Affairs, Karita Bekkemellem, has stated this is an important issue, and will consider to propose new legislation if the banks don't accept responsibility.

Articles in Norwegian:

<http://www.dn.no/privatokonomi/article875204.ece>

<http://www.dn.no/forsiden/politikkSamfunn/article876885.ece>

[Also noted by Tore A. Klock. PGN]

⚡ Risks of reprogrammable ATMs

<msb@vex.net (Mark Brader)>

Thu, 14 Sep 2006 23:18:36 -0400 (EDT)

Surveillance footage on a gas station ATM shows a man swiping an ATM card, punching in a series of numbers, and breaking the machine's security code.

He apparently reprogrammed the ATM to disburse \$20 bills while recording the transaction as a \$5 debit. He then apparently used a prepaid debit card.

The shortfall was not noticed until nine days later, when a customer

reported receiving four times what was requested. [PGN-ed]

<http://apnews.myway.com/article/20060913/D8K496C04.html>

✈ Segway software gives hard landing

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

Fri, 15 Sep 2006 8:59:18 PDT

[Source: Linda Rosencrance, Software glitch prompts Segway recall;

Six injuries reported when transporter unexpectedly reverses direction

Computerworld, 14 Sep 2006, PGN-ed; TNX to Nelson H. F. Beebe, U Utah.]

<http://cwflyris.computerworld.com/t/854524/419952/33869/2/>

Segway Inc. is recalling all of its 23,500 Segway Personal Transporters

because of a software problem that can cause the wheels of the device to unexpectedly reverse direction and cause a rider to fall.

Consumers should stop using the device immediately and contact the company

for a free software upgrade, according to the U.S. Consumer Product Safety

Commission, which is working with Segway on the recall. Bedford, N.H.-based

Segway said no hardware changes are required.

A commission spokesman said Segway received reports of six incidents that

involved facial and wrist injuries. One user required facial surgery and

another was hospitalized overnight. Others suffered broken teeth, he said.

"A condition has been identified in which the Segway PT can unexpectedly

reverse the direction of the wheels, which can cause a rider to fall," the company said today. "This can occur when the PT's Speed Limiter tilts back the machine to slow it down and the rider goes off and then back onto the PT within a short period of time."

The voluntary recall applies to all Segway PTs sold to date, including all Segway PT i Series, e Series, p Series, XT, GT and i2 models. The Segway x2, due for release later this month, is not affected by the recall. All new shipments of the I2 are being shipped with the new software release, the company said in the statement.

[This was also noted by Howard Israel and Jeremy Epstein.]

⚡ Yet Another Power Outage

<"Mike Swaim" <mswaim@mdacc.tmc.edu>>

Wed, 6 Sep 2006 12:27:41 -0500

Here's yet another power outage story that features a failure mode that I don't think has been mentioned yet. Back around 2000 or so, when I was at Enron, we lost power to most of the production database servers used for gas and power trading. Only the servers were affected, and the power outage wasn't caused by the failure of anything electronic.

The raised floor under the power director feeding the servers collapsed. When the director sensed the sudden motion, it immediately shut off, taking

all of the servers with it. After a couple of hours it was jacked back into a level position, and turned back on, bringing everything else back to life.

That weekend the floor was repaired.

Mike Swaim swaim@hal-pc.org

MD Anderson Dept. of Biostatistics & Applied Mathematics

mpswaim@mdanderson.org or mswaim@mdacc.tmc.edu at work

⚡ Careful with that Fedex account number

<Matt Wilbur <matt@efs.org>>

Wed, 20 Sep 2006 10:45:49 -0700

Sending packages with Fedex is now easier than ever, thanks to the fedex.com website. Unfortunately, it's too easy. In most cases, if you know a company's account number, you can send whatever you like using the site, assuming you have a pulse, a browser, and access to the Internet.

We recently had an angry ex-employee use our account number to send multiple small dollar amount packages all over the place. The dollar value was too low for the authorities, and it was really just a nuisance. Our "Fedex person" called Fedex to stop this, and customer service told her the only way was to change our account number. This would be painful, so we sent him letters telling him to stop. It didn't. We called Fedex again, this time asking for security, using words/phrases like "fraud," "theft," and "you will have to pay when we reverse the charges." We didn't get

anyone from
Security, but they did begin to listen.

After being bounced around at fedex, we learned the following:

* Unless you take specific action (enable and configure Shipping Administration for your account within Ship Manager on the website),

anyone on the planet can create a fedex.com account, associate it with

your account number, and ship whatever, wherever they way, third party included.

* there is no way, even with shipping administrator, within fedex.com, to

view the logins associated with your account. We had to call and insist on

a list - for "security" reasons they could not email or otherwise send us

a list, but were able to tell us logins, names, last login, and email of active accounts.

After setting up Shipping Administration, we verified that this ex-employee

(or anyone else we don't approve) can no longer set up a new login and associate it with our account.

After about an hour on the phone, we were able to get his login deleted (and

learn all of this additional information about their system).

Risks? For Fedex? Not defaulting to a more secure configuration (like, want

to use fedex on the web? First sign-in associated with that fedex account

must set up "Shipping Administrator" to prevent unauthorized use). Building

an application with all the shipping capabilities imaginable available, and

very little for the account holder to manage access and

security. Not having a security contact or phone number listed, or accessible by calling in to customer service. Money lost to fraud by abuse of this system.

For the Fedex user? Giving your fedex account number to third parties who may ship things to you, unless you know and trust them, and trust their handling of your account number. Not watching your bills closely. Signing up and using for a service that, when you think about it, is far too easy to use to have any built-in safety.

🔥 Hotel minibar keys open Diebold voting machines

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

Thu, 21 Sep 2006 9:47:01 PDT

The access panel door on a Diebold AccuVote-TS voting machine --- the door that protects the memory card that stores the votes, and is the main barrier to the injection of a virus --- can be opened with a standard key that is widely available on the Internet. ... we did a live demo for our Princeton Computer Science colleagues of the vote-stealing software described in our paper and video. Afterward, Chris Teng, a technical staff member, asked to look at the key that came with the voting machine. He noticed an alphanumeric code printed on the key, and remarked that he had a key at home with the same code on it. The next day he brought in his key and sure enough it opened the voting machine.

See Ed Felten's blog:

<http://www.freedom-to-tinker.com/?p=1064>

✶ Cuyahoga County Primary Election Report

<"David Leshar" <wb8foz@panix.com>>

Sun, 17 Sep 2006 17:01:11 -0400 (EDT)

Cuyahoga County [which includes Cleveland] had a major meltdown in their May 2006 primary election. A Review Panel [comprised of a local judge, the head of the Ohio Lottery, an academic, with local law students as staff] issued a report on the event, and what needs to be fixed.

<http://www.votingintegrity.org/pdf/cerp_rpt06.pdf>

While Diebold DRE machines are deeply embedded in the debacle, the report is not about the problems with machine's security [as Ed Felten's is] as much as the issues of acquiring, configuring and deploying them.

The Road To Hell is paved with good intentions, and this report has asphalt enough to go around. It's an example of how you can you can make any problem too hard to handle if only there is enough money & patronage floating around...

RISK readers can easily identify all the Usual Suspects; you could almost duplicate it with cut and paste from say, DIVAD/Sergeant York, Virtual Case File, and oh the Second Ave subway project escapades. Cuyahoga County Board of Elections says they were told they were buying, from the sole

source
vendor, "seamless integration" between the registered voter
database and
ballot creation processes; while the vendor was seemingly
wearing hooded
white robes. [Diebold bought the West Coast voter database
company but it
was still a separate operation who {oops} wanted to be paid
extra for their
added work; work allegedly never mentioned by the corporate
salesman who
sold the "seamless" package to the BoE.]

The BoE didn't even have the authority to spend the money they
thought was
"theirs" and thus never asked the County Commissioners.

It also touches on the very real issue of poll workers/election
day
staff. Elections are transient events, and many of the polling
places are
likely to be staffed by people not just with little or no
computer
experience; but often computerphobia. Add training problems and
you have a
disaster brewing.

There are VERY few Avi Rubin's working at polling places; and
outside of
Silicon Valley, I bet do no more than start Word. I wonder how
many RISK
readers do so? I'm almost tempted to say there should be
Election Day Duty
al-la Jury Duty. For now, employers could show their support by
encouraging
both senior staff & IT support to volunteer. Both would get a
valuable
reminder in Real World 101.

The only good aspect is the Ohio Legislature required honest-to-
gosh paper
as the ballot of record. While that makes jammed printers
important, it

means there is something to recount when, not if, things go wrong...

✈ **Re: Avi Rubin's latest report as an election judge**

<"Kurt Fredriksson" <kurt.fredriksson@ieee.org>>

Wed, 13 Sep 2006 23:50:08 +0200

I'm a Swede and is a bit puzzled about the eletronic voting that seems to become so popular in the US.

As we are going to have a general election this sunday (sept 17), I can't help making a comparison.

The precinct Avi was reporting from had over 1000 voters. The precinct I am going to use this sunday has around 1200 voters of which around 1000 usually show up. Thus quite similar in size.

Avi had 12 machines and 16 judges, opening hours 0700 - 2200, long queues.

We have no machines (old fashion paper ballots) and 3 + 3 layman officials, opening hours 0800 - 2000, no queues.

After 2000 (8 pm) the votes for the the Swedish Parliament are handcounted at the precinct in the presence of all interested. That takes about one hour. These results are then telephoned to the central authority. All votes are then recounted a couple of days later, to get the official result. This recount is also performed in the presence of all interested. All votes are

kept in sealed and secured boxes during transport.

What are the advantages with electronic voting? Reading Avi's blog makes one wonder.

SSN-as-ID under scrutiny - again

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>

Tue, 12 Sep 2006 08:08:11 +0200

The insecure method of trying to use a verbal report of a U.S. Social Security Number (SSN) as personal identification is coming under wider scrutiny because of the brouhaha about the Hewlett-Packard board. The Chairman apparently ordered an investigation into who was giving privileged information to news media, and the investigators hired pretexters to obtain phone records of board members.

Pretexters are people who use "social engineering" skills to impersonate a third person while communicating with a service provider, in order to obtain information about the services provided to that person. In this case, the pretexters wanted to obtain the telephone-call records of HP board members.

The International Herald Tribune recounts the practice at <http://www.iht.com/articles/2006/09/11/business/hpspy.php> in a story from the New York Times by Matt Richtel and Miguel Helft. One investigator who helps auto-repossession agencies demonstrated:

"In most cases [the investigator] said, he already had the Social Security number from the lien holder. But if necessary, he could find it in commercial databases. To demonstrate, he asked a reported his full name and state of residence, and read him back his Social Security number within seconds." [op.cit.]

Among companies who have adapted belatedly to this reality are Verizon, who apparently stopped using SSN as "a chief way to establish [a customer's] identity" last year. Among those who have not yet adapted are AT&T, which "[continues] to accept Social Security numbers as a central means of identification."

The article discusses the legality of pretexting, which may already be generally illegal in many jurisdictions and is so for particular goals such as obtaining financial records, and efforts to make it more explicitly illegal. The legality of pretexting is obviously a different issue from the insecurity of authentication through SSN, just as the legality of thievery is a different issue from whether I lock my front door when I leave the house.

It has been known for years, and not just to RISKS readers, just how dysfunctional the practice is of trying to authenticate people through basic information such as residential address and SSN. Perhaps it persists because the perpetrators (service companies) are not the sufferers (their customers). There is, however, a general legal notion of "due

diligence",
whereby if a company uses a method which is known to be
ineffective, it can
be held responsible for deleterious consequences, as having not
exercise due
diligence. So, when it becomes sufficiently "well known" that
divulging SSN
is ineffective as authentication, practice could change. The HP
story might
help to tip the scales.

Peter B. Ladkin, Causalis Limited and University of Bielefeld
www.causalis.com www.rvs.uni-bielefeld.de

⚡ New way to break into cars

<Gerrit Muller <gerrit.muller@embeddedsystems.nl>>
Tue, 12 Sep 2006 10:08:55 +0200

Dutch media report on a new way thieves are using to break into
cars with
electronic locks, see for instance:
[http://www.rtvnoord.nl/nieuws/index.asp?
actie=totaalbericht&pid=60184](http://www.rtvnoord.nl/nieuws/index.asp?actie=totaalbericht&pid=60184)

In Stadskanaal, in the North of the Netherlands, at least 30
cars have been
illegally opened without any trace or damage. Thieves appear
mostly to look
for car documents. The police don't have any clue how the cars
have been
opened. One of the possibilities being looked into is the
existence of some
new electronic device acting as a passkey.

If such an electronic passkey would exist, then we see the next
phase in the
(electronic) security rat-race.

Gaudi systems architecting <<http://www.gaudisite.nl/>>

⚡ Thieves sabotage telecom infrastructure

<Gerrit Muller <gerrit.muller@embeddedsystems.nl>>

Tue, 12 Sep 2006 10:02:29 +0200

Several Dutch media report the sabotage of telecom infrastructure at a business park in Blerick, near Venlo, in the South of the Netherlands, e.g.,

http://www.telegraaf.nl/binnenland/49777581/KPN_heeft_handenvol_aan_gesaboteerde_kastjes.html

In Blerick the cabinets of KPN (Dutch Telecom provider) were broken down.

Apparently the inflictors wanted to eliminate the security of businesses at the park. They succeeded and stole for 100k's Euro's from DHL, the courier company.

The same attempt was made at the business park in Herkenbosch, another small town in the South. However an attempt to break in at an attraction park here didn't succeed, because the alarm was still functional.

This example again illustrates the often invisible dependencies of modern interlinked systems. Many modern security services depend on public infrastructure. How many of them have these single points of vulnerability?

✶ Cops say teen concocted radio calls

<"S Hutto" <shuttoj@gmail.com>>

Mon, 11 Sep 2006 22:01:31 -0600

Westword, a Denver area weekly, has published a long article on the teen who was arrested for impersonating an officer on local police radio bands in 2001. According to the article, he had been routinely communicating on police bands for about three months, requesting licence plate checks and once reporting a fake hit-and-run accident. He was found guilty and sentenced to six months in the Division of Youth Corrections and two years' probation. The article provides some mundane technical details on the incident. RISKS readers may be interested in the somewhat dramatized events and motivations that drove the teen to impersonate a law enforcement officer. In 2006, he was arrested and charged with impersonating an EMT and theft by receiving.

The article will be available for some amount of time here:

<http://www.westword.com/Issues/2006-08-31/news/feature.html>

✶ Regarding High-tech Product Sabotage (Mellor, [RISKS-24.41](#))

<Phil Singer <psinger1@chartermi.net>>

Wed, 06 Sep 2006 20:17:39 -0400

During the early 1980's the place I worked at had a Honeywell-

compatible
version of the venerable IBM 1401. It came in several models (I
don't
remember the model numbers - call them Model A for the lowest
end up to
Model D for the top end). We found out the hard way that the
only
difference between them was one resistor - take it out and a
Model A was as
fast as a Model D (but leased for tens of thousands less). Our
field
engineer did not like to waste time, so he always disconnected
the resistor
when he did his P.M. In fact he hated wasting time so much that
he never
bothered to reconnect it. On one periodic maintenance day, he
was on
vacation and a somewhat more conscientious engineer took his
place. The
resistor was replaced. The director wanted to know why
everything slowed
down. When he found out, he immediately terminated the lease.

[This is indeed an old phenomenon. Long ago, during my Bell
Labs days, I
requested an upgrade for a telephone modem, which was made by
snipping a
single wire with a disproportionate increase in the monthly
rental. PGN]

⚡ **REVIEW: "Computer Security Basics", Lehtinen/Russell/Gangemi**

<Rob Slade <rmslade@shaw.ca>>
Mon, 18 Sep 2006 11:57:20 -0800

BKCOMPSEC.RVW 20060819

"Computer Security Basics", Rick Lehtinen/Deborah Russell/G. T.
Gangemi Sr., 2006, 0-596-00669-1, U\$39.99/C\$51.99

%A Rick Lehtinen
%A Deborah Russell
%A G. T. Gangemi Sr.
%C 103 Morris St., Suite A, Sebastopol, CA 95472-9902
%D 2006
%G 0-596-00669-1
%I O'Reilly and Associates, Inc.
%O U\$39.99/C\$51.99
%O <http://www.amazon.com/exec/obidos/ASIN/0596006691/robsladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/0596006691/robsladesinte-21>
%O <http://www.amazon.ca/exec/obidos/ASIN/0596006691/robsladesin03-20>
%O Audience i- Tech 1 Writing 1 (see revfaq.htm for explanation)
%P 296 p.
%T "Computer Security Basics, Second Edition"

I've been waiting a long time for an updated version of this classic.

"Computer Security Basics" was a pretty accurate name for the first edition.

The book was an overview of many aspects that go into the security of computers and data systems. While not exhaustive, it provided a starting point from which to pursue specific topics that required more detailed study. Such is no longer the case.

Part one looks at security for today. Chapter one starts with 9/11, then talks about various infosec groups, and only then gets to an introduction of what security is, and how to evaluate potential loopholes. The definition points out the useful difference between the problems of confidentiality and availability, and now adds integrity. The distinction between threats,

vulnerabilities and countermeasures is helpful, but may fail to resolve certain issues. Ironically, in view of the title of this section, chapter two gives some historical background to the development of modern data security.

Part two deals with computer security itself. Chapter three looks at access control, but is somewhat unstructured. Malware and viruses receive the all-too-usual mix of advice and inaccuracies in chapter four. Policy is supposed to be the topic of chapter five, but most of the text is concerned with matters of operations. Internet and Web technologies, and a few network attacks, are listed in chapter six.

The prior inclusion of network topics is rather funny, since part three delves into communications security. Chapter seven turns first to encryption, which could be presumed to have applications in more than communications, although it is important in that field. The material on encryption is quite scattered and disorganized, and the explanation of asymmetric systems is probably more confusing than helpful. A lot about networks, a list of network security components, and not much that is useful makes up chapter eight.

Part four turns to other types of security. Chapter nine takes a confused look at physical security, and includes biometrics: as with encryption and communications, the topic that could be related to physical security, but might more properly be dealt with elsewhere. Chapter ten

reviews wireless LANs, mentioning threats, but only tersely listing security measures, with no detail for use or implementation.

The original version of the book was a good starting point for beginners who had to deal with computer security at a basic level. This second edition is a tremendous disappointment: Lehtinen has done a disservice not only to Russell and Gangemi, but also to those relying on this foundational guide. The tone of the first edition may have been too pompous, but the contents were informed by the primary concerns for information security. This update has introduced random new technical trivia, muddied the structure and flow, and reduced the value of the reference overall.

copyright Robert M. Slade, 1993, 2002, 2006 BKCMPSEC.RVW
20060819

rslade@vcn.bc.ca slade@victoria.tc.ca

rslade@computercrime.org

<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

Search RISKS using [swish-e](#)

Volume 24: Issue 44

Tuesday 26 September 2006

Contents

- [German driverless Transrapid maglev train crashes, killing 23](#)
[Debora Weber-Wulff](#) [Martin Virtel](#) [Peter B. Ladkin](#)
- [SCADA Hacks](#)
[Al Macintyre](#)
- [Vancouver Int'l Airport locked down due to software glitch](#)
[Karl Klashinsky](#)
- [TIAA-CREF Payment Delays Because of New Computer System](#)
[Peter D. Junger](#)
- [DVD player, designed for usability?](#)
[Daniel P.B. Smith](#)
- [1,100 Laptops Missing From Commerce Department](#)
[Alan Sipress via PGN](#)
- [Home security system snafu](#)
[Ron Garret](#)
- [RISKS readers as election officials](#)
[Peter-Lawrence Montgomery](#)
- [Ron Rivest's ThreeBallot](#)
[PGN](#)

- [Identities lost in phishing](#)
[Gadi Evron](#)
 - [22nd Annual Computer Security Applications Conference](#)
[Christoph Schuba](#)
 - [Info on RISKS \(comp.risks\)](#)
-

🚨 German driverless Transrapid maglev train crashes, killing 23

<Debora Weber-Wulff <D.Weber-Wulff@fhtw-berlin.de>>

Sat, 23 Sep 2006 09:01:57 +0200

On Friday, Sept. 22, 2006, the German magnetic levitation train Transrapid (running along a 31,8 km long test loop in Emsland) slammed into a maintenance car on the track while traveling at approx. 200 km/h.

Officials have been quick to assure that this was not a technical error -- although how they can know this before even all of the 23 dead had been retrieved from the wreckage is an open question. The cause was quickly put down to "human failure" -- but has not been elaborated on, probably because Germany was in the process of trying to sell a second Transrapid to China.

Since the test loop is built on 4-meter high stilts and runs through a wooded area, a maintenance car runs once in the morning to clean off leaves and twigs that have gathered overnight and have detrimental effects on magnetic levitation.

The local fire departments did appear to have extra long ladders in order to reach the track, but cranes were necessary in order to lift the

maintenance

car off the flattened front part of the Transrapid train.

The train does not have a driver, who might have noticed something on the track and hit the brakes. Officials say that it is impossible to detect something like this, although I know that for rail-bound trains there are actually detectors that will not signal a train to proceed unless the track portion ahead is clear. [Perhaps they don't have signals, since only one train runs on this track? My speculation - dww]

The train does not offer regular service, but rather takes tourists for a fast trip. The passengers at the time of the accident are said to have been workers for a subcontractor.

From the pictures it seems that some sort of slide construction helped people get out of the (intact) back of the train (the blue things in one of the pictures).

The Transrapid has been sold as a collision-free system, because it cannot fall off the track (it wraps around), nothing can cross its path, and two mag lev trains cannot physically use the same piece of track. The maintenance car, however, was **not** maglev equipment. So we again have the case of the system being logically fine if you stay inside the system, but introducing one piece that is from a different context completely changes the situation.

Article (in German):

http://wwwl.ndr.de/ndr_pages_std/0,2570,OID3129340_SPC3131186,00.html

Pictures of the wreck:

http://ww1.ndr.de/ndrde_slideshow/0,2964,OID3132196_SIX0,00.html

Diagram of the track loop:

<http://www.tagesschau.de/aktuell/meldungen/0,1185,>

[OID5938672_REF1_NAV_BAB,00.html](http://www.tagesschau.de/aktuell/meldungen/0,1185,OID5938672_REF1_NAV_BAB,00.html)

Pictures (with captions in German) explaining how maglev works:

<http://www.spiegel.de/fotostrecke/0,5538,PB64->

[SUQ9MTYzNTMmbnI9MQ_3_3,00.html](http://www.spiegel.de/fotostrecke/0,5538,PB64-SUQ9MTYzNTMmbnI9MQ_3_3,00.html)

Prof.Dr. Debora Weber-Wulff, FHTW Berlin, FB 4, Treskowallee 8,
10313 Berlin

+49-30-5019-2320 <http://www.f4.fhtw-berlin.de/people/weberwu/>

[Two other reports follow, and provide some diversity of
views, although

I have trimmed some of the duplications. PGN]

German driverless Transrapid maglev train crashes, killing 23

<"Martin Virtel" <virtel.martin@ftd.de>>

Sat, 23 Sep 2006 11:11:35 +0200

The two workers on the maintenance vehicle saw things coming and
jumped,
saving their lives.

The test track, which is used as a technology showcase and
transports
curious tourists and potential customers of the technology, had
been
approved for driverless operation only last year.

Right now after the accident, engineers assure us that In
theory, maglev
technology is the safest transport in the world, because the
propulsion is
done by magnets in the rail - two maglev vehicles on the same
part of the

track would run in the same direction, so a crash between them is indeed impossible.

Apparently, nobody thought about non-maglev vehicles on the same track, although these vehicles stick around for routine maintenance. Which is really tragic, because railways, a 19th century technology, normally do have the technology to ensure that only one vehicle is on a given part of the track, and they used to have drivers on board as a fall-back.

And, of course, unspecified "human error" is cited as the most probable cause for the accident, the second theory being a disruption of an unspecified wireless communication system.

<http://www.spiegel.de/wissenschaft/mensch/0,1518,438706,00.html>

Martin Virtel, Redakteur Forschen & Entwickeln, FINANCIAL TIMES DEUTSCHLAND

Stubbenhuk 3, 20459 Hamburg +49/40/319 90 469 <http://www.ftd.de>

German driverless Transrapid maglev train crashes, killing 23

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>

Sat, 23 Sep 2006 09:06:58 +0200

The International Herald Tribune (IHT) has a story by Mark Landler of the NYT. Our local paper, the Neue Westfälische (NW) is running a story from the Associated Press (AP).

The IHT says it was traveling about 200kph. The NW says about 180kph.

The IHT is reporting 25 dead and 10 seriously injured. The NW is reporting 23 dead and 10 seriously injured.

The IHT says that "The authorities declined to speculate on the cause, though experts on maglev technology said it appeared to have been caused by a communications breakdown rather than a flaw in the technology." The AP quotes the state lawyer involved saying "it is probably the result of human error." The AP also says that the state justice department and the operating company IABG are assuming it is human error.

It astonishes me that some authorities are willing to speculate in public on the root cause of the crash only a day after it has happened.

The NW said that [my translation] "according to the state legal department, the Transrapid can only travel [on its test track] when the maintenance vehicle has left the track. The maintenance workers confirm this by telephone. it is open [that is, it has not been determined PBL] why the train controller gave permission for the train to proceed."

So let me join in, but without speculating. Any collision between two rail vehicles demonstrates that the means of ensuring that two vehicles are not in the same place at the same time is inadequate. The reason I can say this is because it is an analytic statement: a collision happened, therefore the means of hindering collisions was inadequate. (The classic example of an

analytic statement is that a bachelor is an unmarried man.)

On a single-vehicle short track, one imagines there are lots of economical ways of checking that the track is free which do not involve merely telephone calls. People obviously thought that what they had was adequate. Turns out it wasn't. (Remember: this is an analytic statement.)

Peter B. Ladkin, Faculty of Technology, University of Bielefeld, 33594 Bielefeld, Germany Tel+msg +49 (0)521 880 7319 www.rvs.uni-bielefeld.de

⚡ SCADA Hacks

<Al Macintyre <macwheel99@sigeom.net>>

Wed, 13 Sep 2006 23:44:20 -0500

Infoworld interviewed:

- * Alan Paller, director of research at the SANS Institute, and
- * Eric Byres, director of industrial cyber security at Symantec, on some topics of interest to us.

SCADA (supervisory control and data acquisition) systems, essential to the nation's critical infrastructure, have been hacked.

What's happening today is that terrorists are using cybercrime to get the money to buy the bombs to blow people up. They are not using cyberattacks against physical things. There have been cases where SCADA systems that run power plants, were taken over, but the crime was about financial extortion.

SCADA systems are becoming more vulnerable to cyber attack

because obscure operating systems are being replaced with Windows connected to corporate networks, that are vulnerable to breaches. The GAO did a great report on this in 2004. <http://www.gao.gov/new.items/d04354.pdf>

Then there is the military statement that the Chinese downloaded 10-20 terabytes of sensitive information from NIPRNet.

What the government is doing is producing mountains to reports whose only function is to gather dust. The best thing that can be done with them is pile in front of government buildings as protection against a car bomb.

http://www.infoworld.com/article/06/09/11/37NMmain_1.html

✈ Vancouver Int'l Airport locked down due to software glitch

<Karl Klashinsky <klash@cisco.com>>
Mon, 25 Sep 2006 10:01:42 -0700

On 17 Sep 2006, Vancouver International Airport was locked down for several hours because a security guard noticed what appeared to be an explosive on an X-ray screen. The bag in question could not be located in the screening area, so the decision was made to re-screen all passengers in the waiting areas.

The "lock down" procedure also required many flights that had just taken off to return to Vancouver so that all passengers could be re-

screened.

As it turns out, the bag was not found because it did not exist. The image seen by the guard was from training software installed on the screening machine. The image in question should have appeared only during a training exercise, according to a spokesperson from Canadian Air Transport Security Authority (CATSA). Furthermore:

"They're investigating how that feature of the tool got inadvertently activated. And while they're doing that investigation, they've deactivated the tool itself."

None of the basic facts here will be a surprise to RISKers. However, one thought crossing my mind is whether the training software was executed as a prank, and if so, how (i.e., I have no idea whether it's possible to interact with the screening machines remotely). But if a "false positive" image could be inserted into a live, in-service screening machine, then it's possible that a "false negative" could also be inserted.

The CBC story shortly after the incident, describing the lock down:

<http://www.cbc.ca/canada/british-columbia/story/2006/09/17/vancouver-airport.html>

And the recent story describing the cause:

<http://www.cbc.ca/canada/british-columbia/story/2006/09/22/bc-airport-screening.html>

[Also noted by Robert Israel, UBC, Vancouver]

<http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20060921/>

yvr_security_060921/20060921

✦ TIAA-CREF Payment Delays Because of New Computer System

<"Peter D. Junger" <junger@samsara.law.cwru.edu>>

Mon, 25 Sep 2006 14:34:00 -0400

On 6 Sep I faxed the paperwork to TIAA-CREF requesting a withdrawal from my retirement account expecting that it might take as long as a week before the money was wired to my account. It is now 25 Sep and I am still waiting.

I have spoken to several consultants about this problem. The first just said that it should not have taken that long and that he would see if he could get it expedited. The next consultant was more forthcoming and said that the delay was caused by the fact that TIAA-CREF was installing a new computer system. (I had earlier been told in another context that the old system was written in COBOL back in the 1960s.)

Later consultants told me that as a University's account is transferred to the new system, withdrawal applications from retirees from that University have to be processed manually, rather than by the computer system. That strongly suggests that as more and more accounts are transferred to the new system the delays will get longer and longer.

There apparently has been no public announcement of this problem. (At least

I found nothing in a Google search.) When I mentioned this to one of the consultants, she said that information that there was going to be a switch-over to a new system was sent to account holders last year, but, when I pointed out to her that that announcement said nothing about delays, she said that she did not believe that they had been anticipated.

When I asked what happened to people who couldn't make a mortgage payment or something like that I was told by one of the consultants that TIAA-CREF was reimbursing people who had to pay late charges because of the delay. He didn't say what they did for people whose credit reports were damaged or those who lost a deal because they could not come up with a down payment in time or something like that.

One of consultants also told me that it might be six months before the switch-over to the new system was complete.

The consultants, who were all very considerate, all said that they had no contact the people responsible for the actual processing of the withdrawal applications.

Peter D. Junger, Case Western Reserve University Law School,
Cleveland, OH
junger@samsara.law.cwru.edu <http://samsara.law.cwru.edu>

⚡ DVD player, designed for usability?

<"Daniel P. B. Smith" <usenet2006@dpbsmith.com>>
Mon, 25 Sep 2006 21:06:13 -0400

Look at the button layout on this portable DVD player.

<http://www.dpbsmith.com/buttons.jpg>

In case it still isn't clear--it sure wasn't clear to me--the northeast button navigates east; the southeast button navigates south; the southwest button navigates west; and the northwest button navigates north. The silkscreened little arrows _next to_ each button are apparently intended to convey this, and to help you ignore the engraved little arrows in the buttons themselves.

An awful lot of modern user interface design seems to me to amount to printing little silkscreened arrows next to buttons that were hopelessly misplaced to begin with.

[This of course might reminds us of John Denver's final flight, in which

he thought he had run out of gas on one tank and tried to switch tanks.

The lever positions were UP for both tanks off, RIGHT for the left tank,

and DOWN for the right tank. PGN]

✶ 1,100 Laptops Missing From Commerce Department

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

Fri, 22 Sep 2006 16:11:04 PDT

More than 1,100 laptop computers have vanished from the

Department of
Commerce since 2001, including nearly 250 from the Census Bureau
containing
personal information. This was revealed in response to a
request from the
U.S. House Committee on Government Reform, which is surveying 17
federal
departments about such losses. Of the 10 thus far responding,
Commerce is
"by far the most egregious." This leaves questions about the 7
departments
that have not responded! [Source: Alan Sipress, *The Washington
Post*, 22
Sep 2006; PGN-ed]
[http://www.washingtonpost.com/wp-dyn/content/article/2006/09/21/
AR2006092101602.html](http://www.washingtonpost.com/wp-dyn/content/article/2006/09/21/AR2006092101602.html)

🔥 Home security system snafu

<Ron Garret <ron@flownet.com>>
Sun, 24 Sep 2006 11:26:22 -0700

I swear I am not making this up.

Today I got a call from the company that monitors our home
security system.
They said that they had received a trouble report from our
system. But our
panel said everything was hunky-dory. All the self- tests were
normal, and
the sensor in question was operating properly.

This is not the first time this has happened, so I decided to
escalate.
Long story short: the only plausible theory that anyone has been
able to
come up with is that somewhere in the country another security
system has

mistakenly been programmed with our ID code (the ID codes are assigned and programmed manually) and it is THAT system that is calling in the trouble reports. The central monitoring system uses the self-reported ID codes to identify the system calling in, not caller-id. Therefore (assuming this theory is correct) there is no way to know where the system with the duplicate ID actually is.

I pointed out to them that if this theory is correct then the system with the duplicate ID code is essentially useless, and that if and when the owners of that system learn this they may not be too happy about having paid their monthly fees for essentially no value whatsoever. If a burglar ever breaks into that house (wherever it is) it will appear to the monitoring office that someone has broken into OUR house. The police will be dispatched to our house and we'll be charged for a false alarm. Meanwhile the real burglars will be happily unmolested in some unknown and unknowable location. Furthermore, if a burglar ever breaks into OUR house through the location corresponding to the (evidently) faulty sensor on the house with the duplicate ID they might be tempted to write this off as just the faulty sensor acting up and not call the police.

Even the possibility that such events might result in (it seems to me, IANAL) easily winnable lawsuits now that the company has been made aware of the problem has not motivated them to find a solution as far as I can tell.

RISKS readers as election officials (Re: Lesher, [RISKS-24.43](#))

<Peter-Lawrence.Montgomery@cwi.nl>

Fri, 22 Sep 2006 06:48:33 +0200 (MEST)

I'm a mathematician in Microsoft's Cryptography group. On September 19, during the Washington State primary, I was a King County (Seattle area) election judge. This seemed a good use of my expiring vacation hours.

The pay is about \$115 for working about 6 am - 9:30 pm, with a one-hour lunch break and two 15-minute breaks. A four-hour pre-election training session is also reimbursed. This is more than I've received for equivalent jury duty.

The polling station where I was assigned is supposed to have 14 workers, but only 9 had been recruited. Some of us doubled up to do two precincts. I brought a copy of Avi Rubin's report, but most other judges weren't interested.

For those voting in person, this was the first time they could choose electronic voting (AVU, Accessible Voting Unit) or paper ballots. I was across the room from the (one) AVU but understood you touched the screen to pick a candidate. Supposedly it could (slowly) read the ballot aloud in English or Chinese, for those who are visually disabled. A printed copy of your ballot passed under a glass -- you had to affirm that the

choices

printed there are correct before casting your ballot.

If a voter chose AVU, I (as judge) needed to fill in a form with the voter's name and precinct information. Another judge types this precinct information into the AVU so the voter gets a proper ballot.

Paper ballots could be marked (fill in an oval) and dropped in an Accuvote machine, which checked for consistency (e.g., don't vote for two candidates for same office) and tallied the votes. Before opening the polls, we needed to check that all tallies were zero. The end-of-day counts were printed on the same roll of adding-machine tape. Ballots with a write-in candidate automatically went into a separate cannister beneath the Accuvote machine, so they could be separated at days' end. The County will recount all paper ballots by hand in 4% of the polling places.

The Accuvote machine also checked that a political party (Democratic or Republican) had been declared. Some voters deliberately declined this, not voting for partisan offices. The inspector (= chief judge) had to unlock the Accuvote machine and tell it to allow this ballot.

Many King County voters vote absentee, and there are plans to go fully absentee around 2008. The voter lists supplied To election judges omit absentee voters. The precincts at this polling place had a combined 1500 or so registered non-absentee voters, of which about 250 chose paper ballots and 30 chose AVU (30% turnout. I heard those who used the AVU liked it. There were about 60 absentee ballots dropped off at this polling

place.

Occasionally multiple members of a neighborhood would show up together, and there would be a wait in the line for that precinct. But delays were short -- having only nine workers wasn't so bad after all).

My usual polling place is elsewhere, and I could not access it during voting hours. I cast a provisional ballot, where my name is outside an envelope and the ballot inside. Provisional ballots must be paper. I was able to cast a vote on many judges as well as state legislators, US Senator, and a county tax, but not for US Representative, because my residence is in another congressional district. Several voters who walked in, claiming they had not received their absentee ballot (and were not on our lists), were allowed to vote provisionally.

At the end of the day, many items to be returned to the county were delivered by the inspector, who needed an accomplice of the opposite political party. There were three bags supplied for these items, but it was hard to fit everything in. Some items, such as the privacy booths used by paper voters, were left behind for the county to pick up later.

King County election procedures came under criticism in 2004-2005, while the 2004 gubernatorial election results were being challenged. I saw no severe anomalies Tuesday. A technician stopped by during the morning, to check that things were going well.

⚡ Ron Rivest's ThreeBallot

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

Mon, 25 Sep 2006 15:25:01 PDT

If you have not yet seen Ron Rivest's latest offering, this one is essential reading: a three-part paper ballot that satisfies privacy and integrity while avoiding vote selling and eschewing cryptography. Very clever, very cute. Cheers! PGN

<http://theory.csail.mit.edu/~rivest/Rivest-TheThreeBallotVotingSystem.pdf>

⚡ Identities lost in phishing

<Gadi Evron <ge@linuxbox.org>>

Mon, 18 Sep 2006 06:57:16 -0500 (CDT)

As I often comment, it is funny to me (not really but hold on) when people scream about this or that organization losing a laptop with 20K identities. What's 20K?

Obviously that is important, and speaks volumes of corporate security and of privacy issues. Still, it is insignificant in a laughable fashion when compared to what's being stolen daily online.

Every day, millions of online identities and website credentials are lost. Millions. Every day.

This is done through trojan horses which are spread (bots, worm fashion) among an immense online population. There are thousands of new variants to these bots coming out every month dedicated specifically as a targeted attack on online financial institutions.

These attacks target the financial online sites (banking, eCommerce, etc.) not by attacking them directly on the macro level, but rather by multiple micro-level attacks against their users, en-masse.

These trojan horses (bots) are so advanced, they utilize rootkit technology, and when the user surfs to an HTTPS site, use man-in-the-middle attacks on the machine itself to steal his or her credentials.

These credentials in turn are sent to the remote attackers for further processing.

A lot of money is lost this way. This is a world-wide problem, but it is especially apparent (as the bad guys utilize the data more and more) in, but not limited to, the UK and Europe. In the US this is a growing trend, but it is mostly ignored by the defenders (most are not aware of it) as regular primitive "e-mail phishing" is still the most apparent threat there. This is largely due to US banks still mostly using username and password authentication.

E-mail phishing is important and a large threat, but it is doomed to death (it will still be here 10 years from now, like Nigerian scams are here today, but as a specific threat it will diminish into obscurity.

Phishing today should become the root in a tree called Online Financial Fraud or eFraud. That, friends, is not going away whether in blogs, trojan horses, e-mail or your cell phone.

These trojan horse attacks, as they are located on the user's machine itself, are not stopped by 2-factor authentication, etc. There are things that can be done, but when the security problem is on a remote machine not under the, say, bank's control, there is not much they can do with their current confidence risk assessment systems.

There are solutions, but these are to be discussed another time. It is obvious that one of the biggest problems facing banks, and ESPECIALLY eCommerce sites (without the physical-space presence) is how to establish reputation systems that will provide with a technological risk assesment confidence decision as to how safe it is to work with a remote user.

The web channel is the cheapest and most effective in banking today, and banks will not want to lose it.

We (Alan Solomon and myself) cover some of the market involving this technology and how it works in a recent paper we published in the Virus

Bulletin September edition:

<http://www.beyondsecurity.com/whitepapers/SolomonEvronSept06.pdf>

22nd Annual Computer Security Applications Conference

<ACSAC Distribution Manager <distribution@acsac.org>>

Sat, 23 Sep 2006 16:32:25 -0400

22nd Annual Computer Security Applications Conference (ACSAC 2006)

December 11-15, 2006 - Miami Beach, FL

<http://www.acsac.org>

We would like to invite you to attend this year's ACSAC conference in Miami Beach, FL. We have again created an exciting program organized in three tracks, featuring invited speakers, peer-reviewed technical papers, case studies, tutorials, a workshop, a works in progress session, panels, and plenty opportunity to mingle and network with your colleagues from around the globe.

The advance program is posted and registration is now open:

http://www.acsac.org/2006/advance_program.html

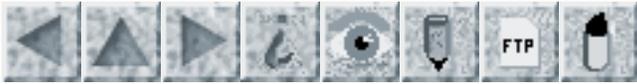
<http://www.regmaster.com/conf/acsac2006.html>

The deadline for securing the early registration discount and hotel room discounts is November 13, 2006.

Dr. Christoph Schuba, 2006 ACSAC program chair Christoph.Schuba@GMail.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

Search RISKS using [swish-e](#)

Volume 24: Issue 45

Thursday 19 October 2006

Contents

- [A380 delivery delays attributed partly to design SW problems](#)
[Peter B. Ladkin](#)
- [More on A380 delivery delays](#)
[Peter B. Ladkin](#)
- [A380 design software incompatibility costs 4.8 billion euros](#)
[Mike Martin](#)
- [Brazil collision: Too much precision a bad thing?](#)
[David Magda](#)
- [The NTSB on John Denver's crash and bad interfaces](#)
[Trammell Hudson](#)
- [More on the Transrapid accident](#)
[Debora Weber-Wulff](#)
- [Transrapid: fault of the people?](#)
[Debora Weber-Wulff](#)
- [Re: Cost of online banking typo put on consumer](#)
[Peter B. Ladkin](#)
- [Identity Theft With Google Code Search](#)
[Gervase Markham](#)

- [AmEx security](#)
[Gregory Marton](#)
 - [2007 Collegiate Voting Systems Competition](#)
[Tim Finin](#)
 - [REVIEW: "World War 3: Information Warfare Basics", Fred Cohen](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈ A380 delivery delays attributed partly to design SW problems

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>

Wed, 11 Oct 2006 09:32:26 +0200

Flight International 10-16 Oct 2006 attributes the wiring-matching problems in the Airbus A380 assembly to problems with design software, reported in an article by Max Kingsley-Jones on p5.

The A380 aircraft has approximately 500 km (300 miles) of internal electrical wiring, which is aluminium rather than the traditional copper. It has been widely reported that the wiring harnesses on body parts fabricated in Hamburg, Germany did not match those of their neighbors built in France when they were mated in Toulouse. This has led to extensive delays in delivery dates, culminating in the resignation both of the former Airbus chief, Gustave Humbert, a few months ago and now his successor, Christian Streiff, this week, as well as the resignation of EADS co-chief Noel Forgeard, who as Airbus chief was largely responsible for the initial development of the A380.

Airbus is forecasting that full production will not be achieved until 2010, and that only 39 A380 aircraft will be delivered by the end of 2009, "compared with 107 originally planned and 80 anticipated under the rescheduling announced in June 2006." The 68-aircraft shortfall is reported by Kingsley-Jones to be worth USD 19 billion in lost revenue, based on a list price of USD 282 million each (note: it is believed that few aircraft sales take place at list price).

Airbus claims to have underestimated the work required to install (press-speak: "complete the installation of") the harnesses. Kingsley-Jones cites Airbus: "The root cause of the problem is the fact that the 3D digital mock-up [software], which facilitates the design of the electrical harnesses installation, was implemented late and that the people working on it were in their learning curve."

It looks as if Airbus is claiming that the wiring design software was a single point of failure. Given what we all know about the risks of developing new SW tools, it seems appropriate to ask why no risk-mitigation measures were put in place as the SW was developed.

Indeed, the former chief executive Christian Streiff sees the problems more generally, reported as saying that Airbus is not yet an "integrated company" and "doesn't yet have a simple and clear organisation".

Peter B. Ladkin, Causalis Limited and University of Bielefeld
www.causalis.com www.rvs.uni-bielefeld.de

✈ More on A380 delivery delays

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>

Thu, 12 Oct 2006 09:07:57 +0200

With respect to the penultimate paragraph in the preceding item, John Rushby pointed out to me that it had been reported that Airbus Hamburg and Airbus Toulouse were using different versions of CATIA software which had incompatible file formats. CATIA is the CAD-CAM software which Airbus, Boeing and Sikorsky, amongst others, have been using for a while. The reports say that engineers in Germany and Spain used Version 4, while those in the UK and France use Version 5, and it is "no secret" (Newton, see below) that those versions are "incompatible at the file format level".

The problems and challenges with using different versions of SW, indeed with data in different formats, are well-known to software managers (if not to almost everyone who has used a PC and tried to upgrade some favorite SW), and Airbus must have had some measures in place to address those issues. Those measures obviously did not suffice. But choosing and evaluating the measures is much more a management issue than a SW issue.

The Bloomberg News story by Andrea Rothman from September 29 is at <http://www.bloomberg.com/apps/news?pid=20601085&sid=aSGkIYVa9IZk> and a technical discussion, including some sensible comments about the situation with company-critical-software updates by Randall S.

Newton at

<http://aecnews.com/articles/2035.aspx>

Peter B. Ladkin, Causalis Limited and University of Bielefeld
www.causalis.com www.rvs.uni-bielefeld.de

[More on the Bloomberg item follows, from Mike Martin. PGN]

A380 design software incompatibility costs 4.8 billion euros

<"mike martin" <mke.martn@gmail.com>>

Wed, 4 Oct 2006 09:46:48 +1000

Bloomberg has reported that the wiring problems that have delayed A380 deliveries yet again are related to incompatibility between versions of CAD software being used:

<http://bloomberg.com/apps/news?pid=20601109&sid=aSGkIYVa9IZk&refer=exclusive>

... engineers in Germany and Spain stuck with an earlier version of

Paris-based Dassault Systemes SA's Catia design software, even though the

French and British offices had upgraded to Catia 5. That meant the German

teams couldn't add their design changes for the electrical wiring back

into the common three-dimensional digital mock-up being produced in

Toulouse, [Charles] Champion [former head of the A380 program] says. Efforts to fiddle with the software to make it compatible failed,

meaning that changes to the designs in the two offices couldn't be managed

and integrated in real time, he says. ``The situation worsened when

construction and tests of the first A380s generated demands for structural

changes that would affect the wiring. The changes in configuration had to

be made manually because the software tools couldn't talk to each other.''

Catia file formats changed between version 4 and version 5. An initiative has now begun to standardise software tools across the program.

According to the latest report on 3 Oct 2006, cost of the consequent

two-year delay to Airbus is estimated to be 4.8 billion euros.

Emirate

Airlines accounts for 45 of the 159 A380s currently on order and according

to Bloomberg yesterday is said to be "reviewing 'all options'".

If it

Cancels, the whole program could be in trouble,

[http://www.bloomberg.com/apps/news?](http://www.bloomberg.com/apps/news?pid=20601087&sid=aNULET1PwpvE&refer=home)

[pid=20601087&sid=aNULET1PwpvE&refer=home](http://www.bloomberg.com/apps/news?pid=20601087&sid=aNULET1PwpvE&refer=home).

While there has been no statement about the reason, the fatal decision to

not upgrade software in Germany and Spain may have been taken so as to avoid

delay to the schedule.

✈ Brazil collision: Too much precision a bad thing?

<David Magda <dmagda@ee.ryerson.ca>>

Fri, 6 Oct 2006 22:20:12 -0400

In light of the recent mid-air collision in Brazil, Philip Greenspun posted

an article to his weblog where he suggests that too much precision in

navigation can be a bad thing.

It's fairly short so I've 'reprinted' it below (which his CC license allows :):

The recent mid-air collision in Brazil of a new regional airliner (fitted out for use as a business jet) and a Boeing 737 has people baffled. How could two brand-new airplanes with advanced avionics, flown by two professional pilots in each plane, collide at 37,000 feet? The precision of modern avionics may well have contributed to this collision.

Airplanes under instrument flight rules fly from one navigation beacon to another along published standard routes. In the old days, with radio navigation receivers and pilots flying by hand, a plane wouldn't fly its clearance exactly. The airways include a tolerance for error of +/- 4 miles. If you're 4 miles to the right of course, in other words, you're still legal and safe from hitting mountains or other obstacles. Altitude was similarly sloppy. If you reached for a drink of coffee or to look at a chart, you might drift up or down 200 feet. Air traffic control wouldn't get upset.

How does it work now that the computer age has finally reached aviation?

The GPS receiver computes an exact great circle route from navaid to navaid.

All GPS receivers run from the same database of latitude/longitude

coordinates, so they all have the same idea of where the Manchester, New

Hampshire VOR is, for example. The autopilot in the plane will

hold the
airplane to within about 30 feet of the centerline of the airway
and to
perhaps 20 feet in altitude. If two planes in opposite
directions are
cleared to fly on the same airway at the same altitude, a
collision now
becomes inevitable.

Almost any other system would be safer. If you sent airplanes
up to fly in
random point-to-point paths, e.g., from Boston to Denver, they'd
be less
likely to encounter one another. If you kept the airway system,
but
introduced some slop into the avionics so that planes always
flew 1 mile to
the right of an airway and + or - 200 feet in altitude, they'd
be less
likely to encounter one another. If you replaced the precise
autopilots
with imprecise humans, planes would be less likely to encounter
one another.
If you replaced the high- precision GPS receivers with low-
precision VOR
receivers, planes would be less likely to encounter one another.

<http://blogs.law.harvard.edu/philg/2006/10/06/mid-air-collision-in-brazil-when-precision-kills/>

⚡ The NTSB on John Denver's crash and bad interfaces

<Trammell Hudson <hudson@osresearch.net>>

Wed, 27 Sep 2006 10:02:28 -0400

> An awful lot of modern user interface design seems to me to
amount to
> printing little silkscreened arrows next to buttons that were

hopelessly
> misplaced to begin with.

I was a guest once at a hotel with a TV remote that had the entire silkscreen worn off from too much use. Luckily none of them were "Buy now" or anything that cost more than a few minutes of frustration. Taking this idea to an extreme, the Das Keyboard makes a fetish out of it by removing all labels from the keycaps to create a totally black keyboard.

Apropos the John Denver crash:

> [This of course might reminds us of John Denver's final flight, in which
> he thought he had run out of gas on one tank and tried to switch tanks.
> The lever positions were UP for both tanks off, RIGHT for the left tank,
> and DOWN for the right tank. PGN]

The NTSB report Probable Cause listed the switch orientation as a contributing factor, but the primary one was the switch location behind the pilot seat. The NTSB found that "when investigators attempted to switch fuel tanks in a similar Long EZ, each time while an investigator turned his body the 90 degrees required to reach the valve, his natural tendency was to extend his right foot against the right rudder pedal to support his body as he turned in the seat."

As reported in [RISKS-20.43](#), the original builder of the rear engined experimental aircraft deviated from the designers plans, and selected the non-standard location to avoid having any fuel plumbing in the cockpit. A good idea, perhaps, but one with plenty of other repercussions.

More on the Transrapid accident

<Debora Weber-Wulff <D.Weber-Wulff@fhtw-berlin.de>>

Tue, 26 Sep 2006 19:37:44 +0200

Spiegel-Online reports on the "Stone-Age" technology used for security on

the Transrapid test track:

<http://www.spiegel.de/panorama/0,1518,439302,00.html>

Characteristic for a number of other unnamed technology is the record of the communication between the central control and the cars.

[Other reports have said that normally the oral command to proceed is given only after the controllers have seen that the maintenance car is in its dock (it is with sight of the tower) *and* they have spoken with the operators.]

The communication record (sort of the black box of airplanes) is recorded on 8-track tapes. The tapes in use have been used over and over again and are almost not audible. The system also tries to "optimize" the tape use by storing every transmission on the "next free track" which is not necessarily the $n+1$ th mod 8 track. There is no time stamp, so the investigators will have to piece together a puzzle of almost inaudible bits of communication, trying to figure out exactly what happened.

It appears that the investigators have no 8-track playing equipment in all

of Germany and are asking for international help. [Mine died *years* ago! -
dww] The first order of business will be trying to make a copy of the tape,
because they are fearful of destroying it by replaying it too much.

In another report criticism has been leveled on the security concept for the
transrapid track to be built in Munich.

<http://www.br-online.de/bayern-heute/artikel/0609/26-transrapid/index.xml>

It seems that the concept goes like this [grossly shortened and distorted by dww]:

1. The Transrapid is absolutely secure, no accidents can happen.
2. Not even in a tunnel.
3. So we don't need a fancy security system.

No more detailed reports are expected until the communications can be
deciphered.

Prof. Dr. Debora Weber-Wulff, FHTW Berlin, Internationale
Medieninformatik
10313 Berlin <http://www.f4.fhtw-berlin.de/people/weberwu/> +49-
30-5019-2320

✶ Transrapid: fault of the people?

<Debora Weber-Wulff <D.Weber-Wulff@fhtw-berlin.de>>
Sat, 14 Oct 2006 01:10:49 +0200

The official investigation into the Transrapid crash (a magnetic
levitation
train crashed into a non-maglev service car at approximately 170
km/h,
killing 23 people on 22 Sep 2006) has determined that there is no

"technical" failure behind the crash, but that the fault lies with the trainman in the maglev vehicle (who died in the crash) and the two dispatchers who let the train start although the service train was still on the track.

There were, however, two previous accidents involving the service cars, according to the Tagesschau-online:
<http://www.tagesschau.de/aktuell/meldungen/0,,OID5999452,00.html>

On 10 Dec 2004 two service cars running in opposite directions collided in the fog because of icy conditions. The impact was only at 20 km/h, so no people were hurt, but the collision caused 100,000 euros worth of damage to the cars. At this time the employees of the Transrapid requested additional security precautions, which were denied on the grounds of being an unnecessary expenditure.

In Jan 2005 there was another accident (that has been acknowledged by the state government) in which a service car had an attachment folded down under the track and smashed into one of the stilts the tracks are built on. There were no people hurt in this incident, either.

A speaker for the government insists that everything is fine, these accidents were recorded but not reported, since they were such "small accidents".

An ethical question: even if the company running the train is found to be legally guiltless, shouldn't they have set up some sort of fool-proof

signaling system after that first accident?

Further reports say that a German and an American lawyer are suing Siemens, who are responsible both for the security system of the Transrapid and for the cable car in Kaprun, which caught fire on 11 Nov 2000, killing 155 persons, in the USA because the company has a subsidiary there. (http://www.tagesschau.de/aktuell/meldungen/0,1185,OID5980314_REF_NAV_BAB,00.html)

✉ Re: Cost of online banking typo put on consumer (Homme, [RISKS-24.43](#))

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>

Fri, 22 Sep 2006 05:15:57 +0200

Kjetil Torgrim Homme's account of a mistakenly typed bank account number in an electronic transaction causing a transfer to a third party astounds me.

German banks require not only the account number but also the recipient name to match the account number before they will initiate a transfer. The danger of a typo is largely that the discrepancy will cause an attempted payment to fail, and you will only be informed in time if you print out your account statement shortly afterwards, since German banks issue on-demand statements only. This may well lead to tensions with creditors if one forgets to check.

This same danger has been present in another form for some time.

If one fills out a payment slip by hand, characters or numerals may be misread by the automatic reader, leading similarly to non-payment. German banks do not issue checks (cheques); account-to-account transfers are the usual non-cash means of payment (apart from credit cards, whose use is still not widespread, compared with the US or UK).

Peter B. Ladkin, Causalis Limited and University of Bielefeld,
www.causalis.com www.rvs.uni-bielefeld.de

✦ Identity Theft With Google Code Search

<Gervase Markham <gerv@gerv.net>>

Wed, 18 Oct 2006 12:56:30 +0100

Several blogs [0] have pointed out that Google Code Search can be used to discover vulnerabilities in the indexed code. One can find SQL injection possibilities [1], potential buffer overflows [2] and backdoor passwords [3]. But it's not just security holes in software that you can find.

One particular search I did revealed a file containing a particular person's entire collection of usernames and passwords. It included several banking account numbers and passwords, SSNs for him and his wife, keys for popular software and mortgage payment details. Assuming the passwords hadn't changed since, I had more than I needed to steal all his money and his identity.

Irony of ironies, the file was included, as plain text, in the

source code
package for a "secure password storage" product this person had
written and
posted to the web!

I sent him an e-mail a couple of weeks ago, and he replied
saying that some
of the data was out of date, and he would change the rest. But
it's not easy
to change bank account numbers and SSNs.

The RISKS: testing security software with confidential data;
when working on
software, not keeping the development version and the version
you use
separated.

[0] <http://www.kottke.org/06/10/google-code-search>

[1] <http://www.google.com/search?q=inurl:%22SQL+select%22+inurl:asp>

[2] <http://www.google.com/codesearch?q=buffer+%22should+be+big+enough%22>

[3] <http://google.com/codesearch?hl=en&lr=&q=%22backdoor+password%22+%28warning%7Cshell%29>

AmEx security

<Gregory Marton <gremio@csail.mit.edu>>

Fri, 13 Oct 2006 17:45:07 -0400 (EDT)

Somehow I forgot the password I reset recently on my American
Express Blue
Cash card. I thought I knew it, and figured I mistyped it,
because it's a
somewhat strong password, so I entered it three times and got
"locked out".

This turns out to mean that they asked me for my four- to eight-

digit

"secure code". These are inherently less secure than the normal password, so I'm in the habit of generating a random number and forgetting this, but out of curiosity I also tried this three times, just to see if it would really lock me out. Why do so many services use these?

I was soon told to call customer service, who asked me about the card number and the cvv on the card, my name, and one prior address. Now my current address is easily available, and my prior addresses are a matter of public record, as they warned me, and easy to discern if you know some basic facts about me, so it's apparently appallingly easy to pretext me.

At this point I was given a temporary password with which to log in and change my real password, so far so good. They also asked me to set my "secure" number. I asked if I could change that on the web site. No. I asked if they could put me through to something I could type it into. No. I had to reveal it to the representative, and the representative encouraged me to label it, e.g. as mother's birth date, etc. Random numbers away!

So there's no security in a procedure you can circumvent with insecure information, but at least their normal password procedure appears relatively strong, so I thought perhaps it won't take *too* much convincing or education. I reset my normal password, only to be told:

"You Have Successfully Changed Your Password
Please record your new Password."

Thanks, AmEx. Good advice!

Gregory A. Marton

<http://csail.mit.edu/~gremio/>

✦ 2007 Collegiate Voting Systems Competition

<Tim Finin <finin@cs.umbc.edu>>

Tue, 26 Sep 2006 21:05:52 -0400

US election systems are in a crisis -- maybe students can find the way forward. In the 2007 Collegiate Voting Systems Competition, student teams will design, implement, analyze, attack and evaluate complete voting system that must have been used in some election, such as one for a student government or organization. Papers describing and analyzing the system will be submitted for the conference and used to select candidates for the final competition. The conference, to be held in Portland in July 2007, will include demonstrations, mock elections, submitted presentations and invited talks. A panel of judges will make awards for the best overall system, best presentation, best attack, and best paper on voting system metrics. VoComp 2007 will be run by UMBC's Alan Sherman with support from the NSF Cyber Trust program and is seen as a way to engage students in nationally important, state-of-the-art security and privacy research projects and course work. More information on the conference, competition, its rules, and an example system is available at <http://vocomp.org/>.

REVIEW: "World War 3: Information Warfare Basics", Fred Cohen

<Rob Slade <rmslade@shaw.ca>>

Wed, 11 Oct 2006 10:38:21 -0800

BKWW3IWB.RVW 20060823

"World War 3: Information Warfare Basics", Fred Cohen, 2006,
1-878109-40-5

%A Fred Cohen fred.cohen at all dot net

%C 572 Leona Dr, Livermore, CA 94550

%D 2006

%G 1-878109-40-5

%I Fred Cohen and Associates

%O 925-454-0171 all.net

%O [http://www.amazon.com/exec/obidos/ASIN/1878109405/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/1878109405/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/1878109405/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/1878109405/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/1878109405/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/1878109405/robsladesin03-20)

%O Audience n+ Tech 2 Writing 2 (see revfaq.htm for
explanation)

%P 314 p.

%T "World War 3: Information Warfare Basics"

Chapter one asserts that world war 3 is not what most people think it is or will be, and that it is going on right now. (There is also a fairly extensive biography of Dr. Cohen.) A definition of information warfare (or iwar) is the province of chapter two. Cohen starts with the notion that warfare itself is a high-intensity conflict, and then notes that iwar is the manipulation (and protection) of symbolic representations used

by the participants in such a conflict. Numerous instances and examples of iwar are explored, and the definition certainly fits all the forms noted. At the same time, it must be said that the definition, while comprehensive, does not appear to assist in formulating responses to the problem. (The mention of marketing as a form of low-intensity iwar is intriguing. I recall a conversation, with an ex-employee of the CIA, as it happens. This person had just encountered the proposal that advertising agencies deliberately used, and reinforced, certain symbols that were associated with specific meanings and emotions. Being part of the direct target audience he had never noticed the practice while I, as an outsider, was just far enough away from the central culture to have observed it for years.) Cohen finally points out that we are all at war, on an information level, with everyone else.

Chapter three examines the intensity levels of iwar. The information warfare capabilities of numerous nations, and relative comparisons between various groups, are analyzed in chapter four. Cohen also makes a case for China overtaking the United States as a world leader in this regard. (This seems to have the strongest relationship to the subtitled admonition that "we are losing" the world war 3 that we didn't even know was being fought. However, if so, it seems in some contradiction to statements, in chapters two and three, that "we" are all fighting each other, or that "we" are all

in this together.) Criminal activity is reviewed in chapter five, but the material is relatively weak in regard to iwar. The relationship between preaching (especially the dogmatic and extreme forms) and propaganda is clear, so chapter seven's association between religion and iwar is not surprising, but the text does not support the contention in any detailed way. Corporate public relations and business intelligence is discussed in chapter seven. (Of particular interest are the sections on companies against nations and religions.)

Chapter eight analyzes propaganda, not only in terms of the component parts, but also in regard to effective countermeasures. Politics, and the various forms of iwar inherent in it, are in chapter nine. Gaming and game theory have been used in warfare and politics for years, and are examined in chapter ten. Chapter eleven looks at electronic warfare, in many of its forms. Information attack tactics, in chapter twelve, repeats procedures that are well known to those dealing with intrusions and penetration testing. Legal issues associated with iwar are outlined in chapter thirteen. Chapter fourteen deals with broad categories of defences that can be mounted against iwar activities. Education is one, and chapter fifteen examines various forms of education that are necessary for effective protection. Finally, in chapter sixteen, Cohen returns to the concept that all of us need to know about information warfare, and to be on guard against it.

Ultimately, this book is not about World War Three, but about the information warfare, at all levels, taking place around us every day. While more personal and not as academic as Denning's "Information Warfare and Security" (cf. BKINWRSC.RVW), Cohen's work is, in its own way, just as important, since it addresses the types of propaganda to which almost everyone is subject, likely without being aware of it.

copyright Robert M. Slade, 2006 BKWW3IWB.RVW 20060823

rslade@vcn.bc.ca slade@victoria.tc.ca

rslade@computercrime.org

<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

Search RISKS using [swish-e](#)

Volume 24: Issue 46

Sunday 5 November 2006

Contents

- [Recent RISKS hiatus](#)
[PGN](#)
- [Widespread European power failure](#)
[PGN](#)
- [Rail network faces unlimited fine over 16 safety breaches](#)
[Scott Peterson](#)
- [VCR gets wrong time as DST ends](#)
[Steve Golson](#)
- [Three of Australia's major railway routes are blocked](#)
[M. Hackett](#)
- [Computer failure causing A320 PA not to work...](#)
[James Hughes](#)
- [SSE delay and failures reported](#)
[Martyn Thomas](#)
- [Regulating Search Engines? - Calif. Initiative For Internet Privacy](#)
[Lauren Weinstein](#)
- [Several backlogged items from Lauren Weinstein](#)
[PGN](#)

- [Electronic voting blamed for Quebec municipal election 'disaster'](#)
[Dan Hurley](#)
 - [Re: More on A380 delivery delays](#)
[David Smith](#)
 - [Re: A380 design software incompatibility costs 4.8 billion euros](#)
[Ed Prochak](#)
 - [REVIEW: "Writing Secure Code", Michael Howard/David LeBlanc](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Recent RISKS hiatus

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

Sun, 5 Nov 2006 11:12:24 PST

I always regret long gaps between RISKS issues. However, the past two weeks involved attending OOPSLA in Portland OR (with a widespread power failure that triggered evacuation of the entire Convention Center and surrounding area, apparently including stoppage of the light rail system) and the ACM CCS06 in Alexandria VA, along with staying in contact with various activities at work. In both conferences, hotel wireless systems were massively overloaded by the plethora of participants' laptops, with repeated network crashes and process vanishings that made Net access extremely challenging. Herewith is an attempt to catch up with the RISKS backlog.

⚡ Widespread European power failure

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

Sun, 5 Nov 2006 13:17:12 PST

A high-voltage transmission line was shut down over a river to enable a presumably large ship to pass. This is preliminarily being attributed to a propagating outage that affected something like 10,000,000 people in Germany, France, Italy, Austria, Belgium and Spain. [Source: Danna Avsec, Power failure hits Europe, Associated Press, 05 Nov 2006; PGN-ed, TNX to Lauren Weinstein for noting this one.]

http://www.wkyc.com/news/news_article.aspx?storyid=58868

Somewhat ironically, my keynote talk at the ACM CCS 06 included discussions on network-propagating outages in power and telephony, how they keep recurring despite efforts to avoid them, and how they might be prevented.

✶ Rail network faces unlimited fine over 16 safety breaches

<Scott Peterson <scott4@mindspring.com>>

Wed, 01 Nov 2006 08:20:36 -0800

NETWORK RAIL faces an unlimited fine after admitting partial responsibility for one of Britain's worst rail disasters, The company, which owns and operates the entire rail infrastructure, admitted health and safety breaches relating to the accident in October 1999 at Ladbroke Grove. Thirty-one

people died and 400 were injured when a high-speed intercity train crashed into a local service in West London during the morning rush hour.

Network Rail Infrastructure admitted at least 16 infringements at Blackfriars Crown Court, in London. Relatives of three of the victims attended the 20-minute hearing. The charge referred to inadequate signal sighting distances and the obscuring of part of a signal.

Other parts of the charge mean that the company has admitted that it failed to ensure the convening of a signal-sighting committee after equipment was installed in 1995, and also after six incidents when signals were passed when red between 1996 and 1998. In addition, it did not carry out "adequate risk assessments" or investigations following them. [Source: Nicola

Woolcock, *The Times* (London), 1 Nov 2006]

<http://www.timesonline.co.uk/article/0,,200-2431601,00.html#cid=OTC-RSS&attr=Law>

VCR gets wrong time as DST ends

<Steve Golson <sgolson@trilobyte.com>>

Mon, 30 Oct 2006 09:51:36 -0500

My Samsung VCR automatically sets its clock using XDS time signals which are broadcast in my area by WGBH, our local PBS station. The VCR clock has correctly followed DST on and off for years. Yesterday morning after Daylight Savings Time ended, the clock was "automatically" set to the wrong

time, and it read two hours early. Turning the VCR on and off had no effect.

This morning the clock was still wrong. I unplugged the VCR, and when I plugged it back in it displayed "Auto" as it searched the channels for the XDS time signals. Eureka! we have the correct time today.

See also [RISKS-17.73](#), 20.83, 20.95.

Other DST mixups: my new Day-Timer diary for 2007 gives the wrong DST start/stop dates.

Steve Golson / Trilobyte Systems / +1.978.369.9669 /
sgolson@trilobyte.com
Consulting in: Verilog, Synopsys, patent analysis, reverse engineering

✶ Three of Australia's major railway routes are blocked

<"M. Hackett" <dist23@juno.com>>
Fri, 3 Nov 2006 16:03:30 -0800

I am amazed at the number of Australia's single-track rail lines. In the bigger scheme of rail transport in Australia, important lines should all be double-tracked.

It is one thing for NZ to have so many single-track rail lines, as NZ geography can be unduly harsh for the railroad builder.

Canada has this problem to a lesser extent -- as the US rail infrastructure can always be used to route around any multiple trans-Canada

rail snafu.

Canada's rail choke points need to be eliminated, but the central government has not coordinated this yet.

Probably some 30,000 kms of heavily used rail need to be replaced in the next decade in Canada -- but I don't see Ottawa trying to fix this problem either.

See also

http://en.wikipedia.org/wiki/Centralized_traffic_control

http://en.wikipedia.org/wiki/Railway_signal

http://en.wikipedia.org/wiki/Railway_signaling

A huge North American rail safety issue: Dark Track -- tracks without any safety signaling. Canada still has some [due to an incomplete Australian like routing centralization], but the US has literally 'several million KMS' of Dark Track.

On a joules/gram basis -- rail is still in many ways more energy efficient than road transport.

The irony here is that [ideally] coal-steam engines are at best 10% thermodynamically efficient. Diesel-electric trains manage to only stay in the [still dismal] 30% range thermodynamically.

Max Power, CEO

<http://HireMe.geek.nz/>

Derailments cause rail chaos

Three of Australia's major railway routes are blocked this morning because of derailments. The Sydney to Melbourne railway line is blocked between

Junee and Cootamundra in southern New South Wales after a collision between a truck and a freight train last night. Wagga Wagga police say the truck driver was free of the rig before the train hit and no one was injured.

The Olympic Highway is closed near the site and the railway line is expected to be blocked until midday.

In outback South Australia seven derailed freight wagons have been blocking the track near Tarcoola since Wednesday.

The line is an important route between the east coast and Perth, and Adelaide and the Northern Territory.

Today's Ghan service from Adelaide to Alice Springs has been canceled and freight deliveries have been delayed indefinitely.

Yesterday, three rail services were cancelled, leaving hundreds of travelers stranded in Perth, Alice Springs and Adelaide.

Rail traffic in all directions has been delayed.

The Australian Rail Track Corporation expects to clear the line by Sunday.

For more news visit ABC News Online at <http://www.abc.net.au/news>

Catch up with the latest arts and entertainment news in the ABC News

Online blogs Articulate <http://www.abc.net.au/news/arts/articulate/> and

The Shallow End <http://www.abc.net.au/news/arts/theshallowend/>.

✈️ **Computer failure causing A320 PA not to work... [Video]**

<james hughes <James.Hughes@Sun.COM>>

Sat, 21 Oct 2006 13:17:53 -0700

I was on UA 914 from SFO to IAD on October 16th 2006 occupying seat 1B. This is an A320 with a plaque that reads it is the 500th airbus built, with the names of the people that accepted the plane from Airbus to United.

At FL39 approaching Denver, the weirdest thing happened.

It was like a 'B' horror movie.

All of a sudden all the lights in the cabin, including things like seat belt lights, smoking light, call buttons etc. started randomly flashing. The audio system went bonkers also changing channels, alternating static and music, etc... The attached video was taken with my palm cell phone. While this is looking forward, it was even weirder in the back with all the flashing lights.

In the video you can see the lights flashing and the flight attendant trying to get into the cockpit. The PA system flight attendant to cabin and cockpit to cabin did not work. I suspect communications to the cockpit was a problem to judging on how the flight attendant was constantly "ringing the bell" to get the flight crew to open the door...

This went on for 10 minutes. The plane did not descent, turn or otherwise, and even though Channel 9 was not coming through clearly, the

chatter on the
radio was normal.

After it was over, the pilot said later that he was trying to turn off the evacuation alarm(!) which he said was unbelievably loud and sounding in the cockpit (although I did not hear it). He explained that he had never heard this in flight before (good thing) and this was something that they heard in training.

During that 10 minutes he had been in contact with the UA maintenance people.

The explanation was that the passenger control system had failed. He said it was the system that controls the "creature comforts" in the back of the airplane including the lights and toilets (and a bit more I might add! I am a little surprised that the PA, and crew to cockpit communications can be so easily trashed.)

The pilot claimed to have been flying the A320 for 8 years and was taken totally off guard by this.

My kudos to the crew for taking care of this. False alarms are at least distracting, which can contribute to larger issues.

At the end the video, unbelievably, a passenger just had to get up and go to the bathroom really bad. I told him to sit back down, but after the end of the video he went anyway, right in the middle of this mess.

[Video omitted here. Contact Jim to view it. PGN]

SSE delay and failures reported

<"Martyn Thomas" <martyn@thomas-associates.co.uk>>

Wed, 25 Oct 2006 10:15:04 +0100

CRESTCo is the Central Securities Depository for the UK market and Irish equities, and operates the CREST system, which provides settlement facilities for a wide range of corporate and government securities, including those traded on the London and Irish Stock Exchanges.. CREST also settles money market instruments and funds, plus a variety of international securities.

In September 2002, Crestco merged with Euroclear, which provides similar services in other European countries. The merged group decided to develop a single settlement engine (SSE) to unify their technology. Financial News Online reported on October 16th that "Euroclear was due to deliver the first phase last year but it did not go live until May". After the UK Crest system was integrated with the SSE in August, "the platform has suffered from blocked messages, systems instability and slow settlement". The problems have apparently led to a delay in the launch of a system for the Government bonds market that was due on October 23rd.

The October Newsletter from Crestco (available online at <http://www.crestco.co.uk/news/newsletters/newsletter-oct2006.pdf>) describes the problems in some detail.

"On Tuesday, 29 August 2006, a small communications issue between CREST and the SSE late in the afternoon generated a substantial number of error messages. This blocked communication between the systems and effectively halted settlement for a period of time. Although settlement was re-started shortly after 17:00, the result of the delay was that UK banking deadlines were pushed back to around 19:15, with major banks only able to close their systems and process client accounts after 20:00. Additionally, although GBP collateral management processing was fully completed, EUR and USD collateral management (delivery by value (DBV)) events were not run. The issue was caused by a configuration error that was magnified on 29 August 2006 as a result of that date being the record date for coupon payments on a very large number of gilts."

Other reported errors include: "Errors in the automatic splitting processing resulted in securities positions not being split and settled efficiently, leading to clients intervening to assess and manage their securities positions interactively. Unfortunately, the manual splitting process has been running much slower than it should, due to software locking and contention issues similar to those affecting DBV processing. The errors relating to automatic splitting were not identified in testing. However, it is also the case that the erratic problem of settling splits in the wrong order has been difficult to replicate in test scenarios, although CRESTCo

understands why it happens. The locking problems that impacted manual splitting were not spotted in performance testing and, even if present, did not negatively impact overall settlement rates, which are higher than in CREST production. Software changes for the automatic splitting issue are now in place. CRESTCo is also working to improve the performance of the manual splitting process. As with the issue affecting DBVs, this primarily involves 'tuning' and 'balancing' the system carefully, a process that was underway at the time of launch but requires further refinement in the live environment."

I recommend reading the newsletter, which gives an unusually frank description of a private-sector project that has had significant problems.

⚡ Regulating Search Engines? - Calif. Initiative For Internet Privacy

<Lauren Weinstein <lauren@vortex.com>>

Wed, 4 Oct 2006 13:01:47 -0700

Greetings. CIFIP - California Initiative For Internet Privacy (<http://www.cifip.org>) -- is a public effort launched in October 2006 to explore the desirability and possible implementation of voluntary and/or mandated approaches toward improving a range of Internet-related privacy issues. The possibility of legislative actions, including particularly the potential placing of a voter initiative on the 2008 California ballot

dealing with search engine data retention and privacy, are important initial facets of this project.

CIFIP has been founded by Internet veteran Lauren Weinstein, who is based in Los Angeles.

Major Internet search services based in California such as Google and Yahoo! (AltaVista), plus other similar firms with substantial physical facilities located within the state, are routinely collecting vast amounts of data from those persons who conduct searches or perform other operations on these companies' systems. This data frequently includes the details of the searches (that is, the search keywords themselves), connection-related data that can be used in most cases to identify the source of those searches, and other information potentially subject to both internal or external abuse.

Much of this data is intensely personal in nature. Our search requests cover a vast range of topics, including medical and other sensitive queries, business and other research, and for most of us a whole host of searches relating to our personal information, interests, desires, dreams, fantasies, and even fears, among other topics. The outrage over AOL's recent publishing of a vast cache of users' search data served to demonstrate the sensitivity of this data in dramatic fashion ...

For more information, including announcement and public discussion lists, etc., please see:

<http://www.cifip.org>

Thank you for your consideration.

Lauren Weinstein <lauren@vortex.com> Tel: +1 (818) 225-2800

<http://www.pfir.org/lauren>

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

Co-Founder, IOIC International Open Internet Coalition - <http://www.ioic.net>

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

Lauren's Blog: <http://lauren.vortex.com> DayThink: <http://daythink.vortex.com>

✦ Several backlogged items from Lauren Weinstein

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

Sat, 4 Nov 2006 15:54:52 PST

Several additional earlier items from Lauren Weinstein have accumulated

during the recent hiatus. To catch up with the backlog, it seems appropriate to steer you to the original documents rather than include them

here, especially if there is already subsequent discussion on Lauren's site.

Microsoft Plans For Automatic Hobbling of "Pirated" Vista Systems

<http://lauren.vortex.com/archive/000194.html>

Google and Monopolies

<http://lauren.vortex.com/archive/000195.html>

Click Fraud, Google, and Telepathy

<http://lauren.vortex.com/archive/000196.html>

⚡ **Electronic voting blamed for Quebec municipal election 'disaster'**

<"Dan.Hurley" <Dan.Hurley@gov.yk.ca>>

Wed, 25 Oct 2006 10:39:06 -0700

<http://www.cbc.ca/canada/montreal/story/2006/10/25/voting-results.html?ref=rss>

⚡ **Re: More on A380 delivery delays (Ladkin, [RISKS-24.45](#))**

<"David Smith" <d.smith@fnc.co.uk>>

Fri, 20 Oct 2006 09:55:17 +0100

So isn't the real culprit the developer of CATIA who decided to change the file format? If this a Microsoft product wouldn't we all be blaming Bill Gates?

This reminded me of a problem many years ago with the Alsys Ada Compiler.

The company that I worked for used V4 of the Motorola 680x0 compiler on Sun 3/60's, 3/80's etc. Everything was fine until Alsys "upgraded" the compiler to V5. Suddenly the applications that were being developed would no longer work.

After much investigation it was found that Alsys had decided that V5 would use the first page of memory for it's own purposes when the compiled/linked code was executed. We had been using the first page as a vector

table. (Well, that is how I remember it, it was a while ago)

The only solution was to move from Sun/3 hosts to Sun SPARCstation hosts, but as the target was 68040 based and, I think, the V5 compiler had not been validated for such cross development, this was not an option.

This was very nearly the deathknell of one particular product, an Integrated Health & Usage Monitoring System (I-HUMS).

Whose fault was it?

- Alsys for changing the way the compiler compiled?
- Us for using a particular memory architecture?
- Sun for developing the SPARC processor?

David H Smith, Frazer-Nash Consultancy Limited, Stonebridge House, Dorking
Business Park Dorking, Surrey RH4 1HJ UK Tel: +44 (0) 1306 885050

⚡ Re: A380 design software incompatibility costs 4.8 billion euros

<"Ed Prochak" <edprochak@gmail.com>>

Sat, 21 Oct 2006 16:14:22 -0400

Date: Wed, 4 Oct 2006 09:46:48 +1000
From: "mike martin" <mke.martn@gmail.com>
Subject: A380 design software incompatibility costs 4.8 billion euros

Bloomberg has reported that the wiring problems that have delayed A380 deliveries yet again are related to incompatibility between versions of CAD software being used:

<http://bloomberg.com/apps/news?>

[pid=20601109&sid=aSGkIYVa9IZk&refer=ex...<http://bloomberg.com/](http://bloomberg.com/pid=20601109&sid=aSGkIYVa9IZk&refer=ex...)

apps/news?pid=20601109&sid=aSGkIYVa9IZk&refer=exclusive>

... engineers in Germany and Spain stuck with an earlier version of

Paris-based Dassault Systemes SA's Catia design software, even though the

French and British offices had upgraded to Catia 5. That meant the German

teams couldn't add their design changes for the electrical wiring back

into the common three-dimensional digital mock-up being produced in

Toulouse, [Charles] Champion [former head of the A380 program] says. Efforts to fiddle with the software to make it compatible failed,

meaning that changes to the designs in the two offices couldn't be managed

and integrated in real time, he says. ``The situation worsened when

construction and tests of the first A380s generated demands for structural

changes that would affect the wiring. The changes in configuration had to

be made manually because the software tools couldn't talk to each other.''

Catia file formats changed between version 4 and version 5. An initiative

has now begun to standardise software tools across the program.

<end quote>

This incompatibility seems an excuse to me. Surely the French division when

upgrading from version 4 to version 5 of the CAD software had available

conversion software. Given that such software exists, why did they not use

it to integrate the German changes into the central design? It would not

have been "realtime", but it would have shown the incompatibility quickly.

Ed Prochak, Magic Interface, Ltd.

REVIEW: "Writing Secure Code", Michael Howard/David LeBlanc

<Rob Slade <rMslade@shaw.ca>>

Fri, 27 Oct 2006 08:50:21 -0800

BKWRSCCD.RVW 20060910

"Writing Secure Code", Michael Howard/David LeBlanc, 2002,
0-7356-1588-8, U\$39.99/C\$57.99

%A Michael Howard

%A David LeBlanc

%C 1 Microsoft Way, Redmond, WA 98052-6399

%D 2002

%G 0-7356-1588-8

%I Microsoft Press

%O U\$39.99/C\$57.99 800-MSPRESS fax: 206-936-7329

%O [http://www.amazon.com/exec/obidos/ASIN/0735615888/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0735615888/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/0735615888/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0735615888/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/0735615888/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0735615888/robsladesin03-20)

%O Audience a Tech 2 Writing 1 (see revfaq.htm for explanation)

%P 477 p. + CD-ROM

%T "Writing Secure Code"

The introduction states that the purpose of the book is to teach application designers (and particularly .NET developers) to design, write, and test application code in a secure manner.

Part one addresses the contemporary security situation. Chapter

one reviews the need for secure systems. The text is so supplemented by notes, comments, text boxes, and sidebars that it becomes difficult to follow at times. However, ultimately it does have a lot of interesting material that would be useful for those who have to make a case for secure coding practices and processes. Designing secure systems, in chapter two, provides a solid list of secure strategy principles along with details and discussion of them, although much of this deliberation is restricted to "war stories" which are interesting but not always useful. The content makes the point that the mere addition of security technologies does not always make for secure applications, which point is not supported by the inclusion, in the latter part of the material, of a huge list of security technologies.

Part two turns to secure coding techniques. Chapter three details that old standard and nemesis, the buffer overflow. Unfortunately, most of what is provided is limited to code demonstrating that various types of buffer overflows exist, and some contentions in regard to specific C language instructions that should not be used. Code for access control list use on Windows NT4 and 2000 is reviewed in chapter four. Code, but not design, for running with least privilege occupies chapter five. Chapter six is again concerned primarily with source code for cryptographic operations, although limited to pseudorandom number generation (paying insufficient attention to seed values), key management, and miscellaneous topics. Further

functions

involved with encrypting confidential information are in chapter seven.

Chapter eight turns to canonical representation, although the discussion is narrowly confined to filenames and issues of traversal.

Part three concentrates on network-based application considerations even

though network connectivity and access has been given as the reason to pay

attention to secure coding in the first place. Chapter nine looks at the

possibility of port hijacking, and the design of applications in order to

work cooperatively with firewalls. Securing the use of RPC (Remote

Procedure Calls), ActiveX, and DCOM (Distributed Common Object Model) is

covered well in chapter ten, with concepts as well as code and good

explanations (although I know for a fact that accessing dcomcnfg on XP is

not as easy as the authors want to make out). Chapter eleven lists some

denial of service (DoS) attacks and generally suggests limiting the

resources available to applications. Most of the advice on securing

Web-based services, in chapter twelve, boils down to advice not to trust the

client, and various examples of malformed input are described.

Part four contains special topics. Chapter thirteen details .NET functions

and operations related to security, but also provides valuable guidance in

regard to appropriate (and inappropriate) use. Testing of secure applications gets a review of standard procedures, in chapter fourteen, but

the material does not provide an abstract overview of assessment concepts

that could be used to find all possibilities of weakness.

Installation

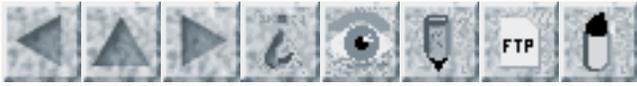
procedures, in chapter fifteen, could have been useful, but is probably the most Windows specific and least practical section of the entire work.

Chapter sixteen is a bit of a grab bag, but contains worthwhile tips and principles to follow (mostly in order to avoid common security pitfalls).

Appendices are usually extraneous material, sometimes added merely to pad out the page count of a book. However, the essays included at the end of this volume could be quite helpful. There are the ten immutable laws of security and the ten immutable laws of security administration, which have become famous in their own right, and have spread through the Internet, as well as a list of dumb excuses given for not doing security properly.

Overall, the book contains much that can be of use for those who wish to develop code that is secure and resistant against bugs and flaws that may open the application to attack. However, there is also a good deal that is irrelevant and not helpful, and a number of issues that could have useful have not been included (such as development methodologies, design strategies, and testing issues).

copyright Robert M. Slade, 2006 BKWRSCCD.RVW 20060910
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<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

Search RISKS using [swish-e](#)

Volume 24: Issue 47

Weds 22 November 2006

Contents

- [More on the European power outage](#)
[PGN](#)
- [Phone service cut to the St. John's region for 5 hours](#)
[Theodore S. Norvell](#)
- [Scottish radiation therapy accident report available](#)
[Richard I Cook](#)
- [Flat train wheels in NY/NJ](#)
[PGN](#)
- [Melbourne's computerised train brakes fail](#)
[Boyd Adamson](#)
- [Yet another canceled public sector IT project](#)
[Martyn Thomas](#)
- [All your eggs... Aegis-class cruiser crippled](#)
[David Lesher](#)
- [Bo Lipari's weblog on election problems: an excerpt](#)
[PGN](#)
- [Some recent election results unresolved -- or unresolvable?](#)
[PGN](#)

- [New Google Service Will Manipulate Caller-ID](#)
[Lauren Weinstein](#)
 - [Proposed Solution For Google's "Click-to-Call" Caller-ID Problem](#)
[Lauren Weinstein](#)
 - [Hospitals Urged to Ease Mobile Phone Rules](#)
[Paul Czyzewski](#)
 - [REVIEW: "Preventing Web Attacks with Apache", Ryan C. Barnett](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ More on the European power outage

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

Mon, 13 Nov 2006 13:11:24 PST

German national electricity network officials issued a formal statement on Sunday morning, in order to announce that a massive power outage that occurred at about 9.30 p.m. on Saturday in the northwestern part of the country, created a domino-like effect in other Western countries as well, such as France, Italy, Austria, some parts of Spain, Portugal, the Netherlands, Belgium and Morocco, immediately after it occurred in Germany.

Officials stated that no less than 82 million German citizens were left without power for almost an hour, while electricity cuts affected around five million French inhabitants as well as the entire northern part of Italy. We weren't very far from a European blackout, one of the managers of a French power company called RTE, highlighted, adding that the failure of

two German high-voltage lines, stretched over a river in north-western Germany - which had been shut down by German utility company E.O.N. in order to let a ship pass through - bear the entire responsibility for the house of cards style European blackouts. In addition to this, the Deutsche Bahn, the national rail company in Germany, announced that 100 regional trains were disrupted by the blackout.

In the past, these operations were often performed with no problems, E.O.N. officials declared in great surprise, while Michael Glos, the German Economy Minister announced the fact that a thorough investigation into the circumstances of this terrible incident is already being conducted: We will examine this report quickly so that together with the companies we can ensure that, if at all possible, such events are not repeated, he stated.

Apart from blaming the Germans for the outage, Italian Prime Minister Romano Prodi stressed upon a more important fact, the need for a stronger electricity policy in Europe legitimated by a powerful authority: It's a rich contradiction that we depend on each other, but we can't help each other without a common authority.

Source: Ruxandra Adam, Softpedia News, 12 Nov 2006

<http://news.softpedia.com/news/Power-Outage-in-Germany-Sparks-Electricity-Collapses-in-Other-Countries-39426.shtml>

⚡ Phone service cut to the St. John's region for 5 hours.

<"Theodore S. Norvell" <theo@engr.mun.ca>>

Mon, 23 Oct 2006 12:31:49 -0230

A small fire led to a power outage at a telephone exchange in St. John's, Newfoundland, Canada on October 20. This led to all phone service in the St. John's region being lost for 5 hours Friday night and Saturday morning. The outage included: 911 service, land lines, Internet, cellular, automated tellers, and point of sale by bank cards and credit cards. Ambulances were dispatched to George St. (the drinking district), "just in case". The loss of 911 service meant that a small child who had stopped breathing had to be transported to the hospital at high speed by her caregivers rather than receiving paramedical attention. Air traffic control at YYT continued to land planes, but could not communicate with ATC elsewhere. Phone service and Internet service is said to have been restored, but my own home phone is no longer working properly.

Those of us who are not familiar with the phone system (and perhaps some who are) are left wondering why a power failure at a single exchange leads to a communications blackout in an entire metropolitan region, and also why all back-up systems failed. Phone service in St. John's is usually quite reliable, even though power failures are quite common in the region, where we get a fair bit of ice, snow, and wind, often all at once. However, this power cut was inside the phone company's building, where it was presumably

downstream of the the back-up generators, but upstream of the back-up computers.

<http://www.cbc.ca/canada/newfoundland-labrador/story/2006/10/23/aliant-fire.html>

Dr. Theodore Norvell, Memorial University of Newfoundland St. John's, NL, Canada, A1B 3X5 +1 709 737-8962 <http://www.engr.mun.ca/~theo>

⚡ Scottish radiation therapy accident report available

<Richard I Cook <ri-cook@uchicago.edu>>

Tue, 31 Oct 2006 09:44:04 -0600

^

[Plus ça change, plus c'est la meme chose.]
)

'Critical error' led to radiation overdoses, scotsman.com

<http://news.scotsman.com/scotland.cfm?id=1596402006>

"...Dr Arthur Johnston, who outlined the devastating chain of events that led to the overdose. His 100-page report pointed out that the Beatson unit had upgraded the computer system it used to calculate radiation doses in May 2005. For the most complex treatment plans, data from the system were transferred to paper forms, as happened in Lisa's case. The report said that the "critical error" occurred when the treatment planner - referred to as Planner B - transcribed the data from the computer to paper, but was unaware of the changes to the system which meant the data were

incorrectly written down. 'The outcome was that the figure entered on the planning form for one of the critical treatment delivery parameters was significantly higher than the figure that should have been used,' the report said. However, the error was not spotted during the checking process and the incorrect dosing information was passed to the radiographer who gave Lisa her treatment. The error came to light only because the same planner made the same mistake in the next plan for a different patient, and this time it was identified by a colleague. An investigation was launched which found that, apart from Lisa, no other patient had been affected. Dr Johnston said Planner B had 'limited experience' and had been under the supervision of an experienced colleague - Principal Planner A - who failed to pick up the error."

Full report available at:

<http://www.scotland.gov.uk/Publications/2006/10/27084909/22>

Dr. Richard I. Cook, Associate Professor, Department of Anesthesia and Critical Care, University of Chicago, Chicago, IL, 60637 1-773-702-4890

Flat train wheels in NY/NJ

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

Wed, 22 Nov 2006 11:03:16 PST

124 railroad passenger cars of the Metro-North Railroad Harlem and Hudson

lines are out of service for at least two weeks. Each fall, oily leaf residue on the tracks tends to cause wheel slippage. Perhaps a la Rube Goldberg, this is interpreted by the circuitry as excessive speed, which causes the brakes to be applied, which causes the wheels to skid, which flattens them out, which affects performance, which causes the cars to be sidelined for wheel truing. The rail yards in New Haven and Harmon can re-true only 9 cars per day, so it is going to take a while to catch up. The newest cars (M-7s) are the ones with the most flat wheels, and operate in pairs, so that one bad wheel takes down both cars. NJ Transit and the LIRR are having similar problems, with the LIRR having to fix 20% of its cars. [This might inspire a step-kick slip-slide in Chorus Line?]

[Source: Caren Halbfinger, 'Flat wheels' deflate train commuters, *The Journal News*, 21 Nov 2006; PGN-ed]
<http://www.thejournalnews.com/apps/pbcs.dll/article?AID=20061121063>

[See [RISKS-7.22](#) and 7.23 for flat wheels at Colwich Junction in 1986, and [RISKS-12.62](#),66,67,73 for the effects of leaves on train tracks in 1991. PGN]

⚡ Melbourne's computerised train brakes fail

<Boyd Adamson <boyd-adamson@usa.net>>
Thu, 16 Nov 2006 09:13:50 +1100

Some of Melbourne's newest passenger trains have had to be withdrawn from service after a spate of braking failures. Connex, the operator of the suburban rail network, has reported 15 incidents involving trains overshooting platforms since 13 Nov 2006 and is at a loss to explain the problem. The most serious incident occurred on Tuesday night when a train failed to stop at Brighton Beach station and traveled into the level crossing at South Road. The boom gates still had not been lowered as the train came to rest in the middle of the intersection. A rail system source said cars were forced to break to avoid colliding with the train.

The problems involve a fleet of 72 German-built trains that were introduced to the suburban network in 2003. Fourteen three-carriage trains have been removed from service following emergency talks between Connex and the trains manufacturer, Siemens. The withdrawal of the trains is expected to cause some disruption to services, particularly on the Pakenham and Cranbourne lines, until the problems can be fixed.

The source said the problems were connected to the trains' computerised braking system. In several incidents, drivers were forced to apply emergency brakes, push emergency stop buttons and activate handbrakes to bring the trains to a halt. But even after activation of all manual braking systems, some trains continued moving. One incident occurred while a driver was undergoing assessment by a transport official. [...]

Since its introduction in April 2003, the Siemens fleet has been

plagued
with controversy. The trains were initially too wide for
suburban tracks and
have recently been repaired to fix faulty wiring. They have also
been
criticised for having only two sets of doors on each side of
each carriage,
causing bottlenecks for passengers.

<http://www.theage.com.au/news/national/brake-woes-sideline-trains/2006/11/15/1163266640138.html>

Yet another canceled public sector IT project

<"Martyn Thomas" <martyn@thomas-associates.co.uk>>

Fri, 27 Oct 2006 12:55:04 +0100

The BBC reports <http://news.bbc.co.uk/1/hi/business/6084454.stm>
that after
four years of development, the UK government has suspended its
plans for an
Internet retirement planner. No date has been set to restart
work on the
proposed service, which was aimed at people on low to middle
incomes.

The online planner was intended to give help to those without
easy access to
financial advice. It would have provided them with
individualised state and
private pension forecasts, and offered advice on how to boost
their
pensions.

Although 11m pounds had been spent on the website, halting the
work will
save the government an estimated 14m pounds. According to the
Minister for

Pensions Reform, James Purnell, the work on the site was halted when the Department for Work and Pensions realised that "delivering accurate online information about state pensions would become increasingly difficult, given the uncertainty about the exact shape of future pension provision".

11m pounds wasted because no-one did a decent requirements analysis?

✦ All your eggs... Aegis-class cruiser crippled

<"David Lesh" <wb8foz@panix.com>>
Sun, 19 Nov 2006 19:31:47 -0500 (EST)

A Usenet poster related that several years ago, for 10 days, an Aegis-class cruiser in the Gulf was crippled by the failure of both of its INS system, and its GPS.

But navigation was not the only issue. It seems virtually all the weapons systems on board require the INS to provide them data on the ships [roll/pitch] attitude to aim/fire. Without such, they are no longer weapons....

Eggs several, baskets one...

Source: Teacher Adam Hilliker gives kid detention for being right
<http://groups.google.com/group/alt.folklore.urban/msg/d8d6c50ef2037625?hl=en>
FoG7h.29214\$nG1.23093@tornado.southeast.rr.com

✦ Bo Lipari's weblog on election problems: an excerpt

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

Fri, 10 Nov 2006 13:54:26 PST

Election Problems, What Election Problems?

Bo Lipari <bolipari@nyvv.org>

Friday, November 10, 2006

The Media Narrative and Public Perception

If you watched the cable news coverage on Election Night, it was easy to come away with the impression that few problems were experienced with electronic voting - the predicted "train wreck" had not materialized. But out in the real world, the HAVA mandated changeover of voting systems resulted in real failures <<http://www.votersunite.org/electionproblems.asp>> that resulted in long lines and lost votes. Just like the fancy new high tech voting machines, the mainstream media has failed us yet again.

That there were widespread problems with electronic voting equipment all around the country is well documented. Thousands of citizens took part in a first time nation-wide effort monitoring polling sites and reporting problems. The reports are still coming in, but it's clear that hundreds and hundreds of problems occurred. But the mainstream media has thus far barely mentioned this, leading one to ask what vast scale of voting disaster would it actually take for the media to report on it?

http://www.votetrustusa.org/index.php?option=com_content&task=view&id=2017&Itemid=26

The Election Night Narrative

News organizations used to report the news, but nowadays they're more concerned with telling their viewers a story. This story, the theme of the day as it were, is called the ``narrative''. On Election Night 2006, the media narrative was ``The Great Tsunami''. The story was about the Democratic tide as it moved from East to West, sweeping away Congress in its path. As soon as the first totals started coming in from the East Coast the news networks started framing everything solely in the context of this narrative. There was no room here for voting machines failures, long lines of voters, or anything else. The story was about the horse race, about devastating loss, about the great wave sweeping across the nation. Voting machine problems had no place here as they would distract from the narrative, even worse, maybe even undermine it. Raising the possibility that votes were lost? How are you going to sell soap with that?

The Unspoken Narrative

Underlying the Great Tsunami story was a subtler narrative, one that the media has consistently fed us on Election Nights for years. This narrative is expressed by the often repeated mantra ``Even if there were problems, it wasn't enough to affect the outcome of the election.''. It seems vitally important to the media that the public believe that no matter what, no

matter how bad the problems, no matter how many lost votes and machine breakdowns, the results are still basically correct, your vote still counts, or at least close enough.

We've been told this story before, in 2000, in 2004, and now again in 2006. Nothing to worry about folks, just a little glitch, pay no attention to the man behind the curtain. This seems to be an essential narrative for the media, one that we must be told and reminded of each and every Election Day. Because imagine what would happen if the media told the public the real story, and showed the real impact on real voters. Why, you might not have just thousands of activists around the country demanding change, you might have hundreds of thousands. If the real story about broken voting machines and lost votes got out, you might even have millions. Imagine, millions of citizens demanding that their right to vote is sacred and not for sale to voting machine vendors, demanding real accountability, demanding accurate elections with results that we can have real confidence in.

Now that would be a tsunami.

<http://nyvv.org/blog/2006/11/election-problems-what-election.html>

⚡ Some recent election results unresolved -- or unresolvable?

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

Wed, 22 Nov 2006 14:04:19 PST

At least five U.S. House races are apparently still unresolved or in question two weeks after the election. I have been waiting for someone else to come up with a retrospective summary and objective analysis of the voting machine problems. Not having found one, I mention just a few of the close races of interest in which the investigation of any of various irregularities could reverse the results.

* Florida 3rd Congressional district, with the peculiarly large (18,300)

undervote for the Sarasota Congressional race in touch-screen machines

that do not permit a meaningful recount (without a new election), with

a computer-reported spread of just a few hundred votes.

This is receiving significant media coverage. Also, see David Dill,

"Is Florida Ready for Democracy?"

http://www.huffingtonpost.com/david-dill/is-florida-ready-for-demo_b_34458.html

[This reminds us of the 210,000 undervotes in the four punch-card counties

in the 1988 Florida Senate race.]

* New Mexico 1st Congressional district, with a .5% difference

* North Carolina 8th Congressional district, with a .025% difference

* North Carolina Court of Appeals, with a .24% difference

[Three other NC elections had very small margins as well.]

* Williamson County, Texas, the votes cast and counted electronically were

each recorded THREE times. (This was detected primarily because the total

number of votes cast exceeded the number of voters.)

⚡ New Google Service Will Manipulate Caller-ID

<Lauren Weinstein <lauren@vortex.com>>

Wed, 22 Nov 2006 15:27:23 -0800

17 Nov 2006, <http://lauren.vortex.com/archive/000200.html>

Greetings. Google has made available a new "Click-to-Call" service that will automatically connect users to business phone listings found via Google search results.

In order for this feature to function, the user must provide their telephone number so that Google can bridge the free call between the business and the user (including long distance calls).

An obvious issue with such a service is that there is no reasonable way to validate the user phone number that is provided. Google says that they have mechanisms in place to try avoid repeated prank calls, but the potential for abuse is obvious.

Of even greater concern is that Google says that it will manipulate the caller-ID on the calls made to the user-provided number, to match that of the business being called. This is extremely problematic, since it could be used to try to convince a prank target that they were being called directly by the business in question, and so cause that target to direct their anger at the innocent business. In the case of targets who are on do-not-call lists, it is possible to imagine legal action being taken by callers upset that the business in question called them "illegally," though in fact the call had been made by the Google system.

Google's explanation for this caller-ID manipulation is that it would be handy to have the called business number in your caller-ID for future calls. That may be true, but the abuse potential is way too high. Caller-ID should never be falsified.

I've written many times about how caller-ID can be manipulated to display false or misleading information, why this should be prevented, and how the telcos have shown little interest in fixing caller-ID or informing their customers about the problem (caller-ID is a cash cow for the telcos whether it is accurate or not).

Up to now, the typical available avenue for manipulating caller-ID has been pay services that tended to limit the potential for largescale abuse since users are charged for access. Google, by providing a free service that will place calls and manipulate caller-ID, vastly increases the scope of the problem. Scale matters.

Google has not vetted this caller-ID feature sufficiently, and I urge its immediate reconsideration.

✶ Proposed Solution For Google's "Click-to-Call" Caller-ID Problem

<Lauren Weinstein <lauren@vortex.com>>

Wed, 22 Nov 2006 15:27:23 -0800

Proposed Solution For Google's "Click-to-Call" Caller-ID Problem, 19 Nov 2006

<http://lauren.vortex.com/archive/000201.html>

Greetings. In a recent blog entry, I discussed my concerns about Google's

new "Click-to-Call" service, especially key issues regarding Google's handling of caller-ID in this service.

Now I'd like to propose a specific solution.

I completely understand why Google likes their caller-ID feature. It's a cute hack (hack in the positive sense), and in the context of non-abusive use brings some value-added. But I really believe that this is one of those cases where somebody needed to get beyond the "gee-whiz isn't this nifty" factor and consider more carefully how it will be abused, particularly on the large free-access scale that Google provides. Even if the vast majority of the calls are legit, the absolute number of abuses is bound to be high, and it seems certain that innocents will be hurt in significant numbers -- there are a lot of jerks in the world who are going to take advantage of this service to get their jollies or take revenge on businesses that they have a gripe with, etc.

However, there is indeed a simple solution in this case. If the caller-ID delivered to both sides of the bridged calls is set to indicate the true source of the calls (i.e., Google) the problem goes away. In fact, caller-ID could be used to further enhance the service by providing a true full point of contact.

What I would do is set the caller-ID to display a Google phone number (ideally toll-free) that played a recorded announcement explaining that the call originated from Google Click-to-Call, and noting how to

proceed (via a Web page, e-mail address, and/or specific phone number) if you felt that you were being targeted for abuse by a user of that system and wanted to file an associated report. This would be a win-win all around. Google would more rapidly get a handle on abusive users, and the service would be even more consumer friendly.

Sometimes there can be a happy ending!

Lauren Weinstein +1(818)225-2800 <http://www.pfir.org/lauren>
PRIVACY Forum - <http://www.vortex.com> Lauren's Blog: <http://lauren.vortex.com>

⚡ Hospitals Urged to Ease Mobile Phone Rules

<"Paul Czyzewski" <tallpaul@gmail.com>>
Wed, 25 Oct 2006 22:46:16 -0700

"The biggest concern is that mobiles interfere with sensitive medical equipment. But a 1997 study from the UK's Medical Devices Agency showed that phones affected just 4% of devices at a distance of one metre, the researchers said."

Who wouldn't want to allow something that affects **only** 4% of sensitive medical devices? The lack of common sense exhibited in the above sentences is mind-boggling. Also, apparently, the phones are classified as only "annoying" as long as they don't actually kill the patient (at least, not

directly).

The "sensible caution" paragraph is mildly reassuring, though somewhat contradictory to the parts quoted above:

"Sensible caution regarding the proximity of mobile phones to medical equipment is thus warranted, but concerns about patient safety alone do not justify zealously enforced no-phone areas, which can cause arguments between staff, patients and visitors."

[Source: Hospitals Urged to Ease Mobile Phone Rules, Reuters, 13 Oct 2006]

<http://www.medscape.com/viewarticle/546041>

⚡ **REVIEW: "Preventing Web Attacks with Apache", Ryan C. Barnett**

<Rob Slade <rMslade@shaw.ca>>

Fri, 03 Nov 2006 11:33:38 -0800

BKPRWAWA.RVW 20060913

"Preventing Web Attacks with Apache", Ryan C. Barnett, 2006, 0-321-32128-6, U\$49.99/C\$66.99

%A Ryan C. Barnett

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario M3C 2T8

%D 2006

%G 0-321-32128-6

%I Addison-Wesley Publishing Co.

%O U\$49.99/C\$66.99 416-447-5101 fax: 416-443-0948

%O <http://www.amazon.com/exec/obidos/ASIN/0321321286/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/0321321286/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/0321321286/>

[robsladesin03-20](#)

%O Audience a- Tech 2 Writing 2 (see revfaq.htm for explanation)

%P 582 p.

%T "Preventing Web Attacks with Apache"

Chapter one notes that there have been many attacks against Web servers and the applications running on them. It also lists the common excuses presented for a lack of security preparation (and assesses the weakness of those arguments). Hardening of the (UNIX) operating system, and network operating system, in order to establish a trusted computing base for the Web server application, are dealt with in chapter two. Initial installation of the Apache software is covered in chapter three. Chapter four reviews the configuration file, and properly secure settings and options. Security related modules in the Apache suite are discussed in chapter five. Chapter six reviews the Center for Internet Security Apache security benchmark tool. The Web Application Security Consortium (WASC) threat classification system is described, in chapter seven, with specific reference to Apache countermeasures against these attacks. (The material provides nice explanations and examples of a variety of exploits.) Buggy Bank, an intentionally flawed e-commerce application that provides practice in hardening a Web server, is outlined in chapter eight. Chapter nine looks at various countermeasures and controls that can be applied to Web servers and sites, noting strengths and weaknesses, and also noting which work most effectively, as well as which can be implemented via Apache functions. If

you'd like to do primary research and gather information on attacks and the level of threat to Web servers, chapter ten details the settings and requirements for using Apache to set up a honeypot server. Chapter eleven finishes off with basic advice on issues such as patch management, and also broadens the discussion to some fundamental concerns in Internet security measures.

A helpful guide for those using Apache.

copyright Robert M. Slade, 2006 BKPRWAWA.RVW 20060913
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<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

Search RISKS using [swish-e](#)

Volume 24: Issue 48

Tuesday 5 December 2006

Contents

- [Still more on the European power outage](#)
[PGN](#)
- [Another power outage brings down German TV station](#)
[Debora Weber-Wulff](#)
- [The UK NHS IT plan](#)
[Brian Randell](#)
- [Rebooting airplanes](#)
[Douglas W. Jones](#)
- [Mascalls, Manchester, what's the difference?](#)
[Mark Brader](#)
- [Three guilty of identity fraud which netted millions](#)
[Brian Randell](#)
- [Identity theft made easy](#)
[John Haselsberger](#)
- [Federal Reserve E-Banking System Outages: Brian Krebs](#)
[PGN](#)
- [How To Tell If Your Cell Phone Is Bugged](#)
[Lauren Weinstein](#)

- [Firefox flaw causes engagement to break off](#)
[Mark Lutton](#)
 - [Critical Firefox hole allows password theft](#)
[Monty Solomon](#)
 - [REVIEW: "Phishing: Cutting the Identity Theft Line", Liniger/Vines](#)
[Rob Slade](#)
 - [REVIEW: "The Security Risk Assessment Handbook", Douglas J. Landoll](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Still more on the European power outage

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

Mon, 4 Dec 2006 14:16:53 PST

More details have emerged on the EON Austria-to-Spain power outage since in

[RISKS-24.47](#) (which erroneously stated rather absurdly that 82 million

Germans were affected, instead of the previously noted 10 million Europeans).

Axel Eble cited the original German text of the E.ON Netz report:

<http://www.eon-energie.com/php/pressemitteilungen/download.php?id=49602>

Jaap Akkerhuis <jaap@NLnetLabs.nl> cited the E.ON report in English:

<http://www.eon-energie.com/php/pressemitteilungen/download.php?id=54598>

The upshot is that the initial calculations for the planned shutdown showed

the link over the Ems River could be compensated for by rerouting alternative power. The so-called "N-1 criterion" for stability was

correctly applied initially, but not reapplied after the reconfiguration.

Thus, the second-order effects of the shutdown were ignored -- namely the increased loads that would result from the rerouting -- and the Norwegian Pearl was allowed to pass.

From the English language version of the report (which explicitly notes that the German version shall prevail in case of any discrepancies), the summary states that "the determination of demands that can actually be met and which the market participants demand of the grid must be continuously be reviewed in a close dialogue between grid operators, grid customers, regulating authorities and political forces." [*]

Continuing from the summary, "Finally, it also remains to be stated that the concrete incident has no connection with issues of grid investments. It must, however, be clearly stated that the growing demands on the grid can only be met -- in the long run -- by a corresponding expansion of the grids."

Once again, we are confronted with the risks of short-term/global optimization.

[* NOTE: As a rather PGN-ish aside, Webster maintains that a "dialogue" can be BETWEEN N entities, where N may be two or more. However, when I learned English, it was customary to make a distinction between "between" and "among" (for N=2 and N>2, respectively). This seems to have fallen by the wayside over time. On the other hand, German uses one word ("zwischen") to cover both, as do French/Spanish ("entre") and Russian ("myeshdu"). At any rate, the concept of a CLOSE DIALOGUE BETWEEN (or even AMONG) N

entities

seems suspect when N is considerably greater than 2, as it is in the

European community, and when communication is inherently NOT CLOSE. I think

that the choice of the German text ("im engen Dialog von ...") is itself

misleading, and that the English translation could have been more accurately

rendered as "in close multipartite communication among ...".

Why do I

engage in such semantic blather? Because the lack of CLOSER COMMUNICATION

is often a serious source of risks in many RISKS episodes, and Conway's Law

and generalization thereof keep resurfacing as representative of fundamental

problems that arise from restricted communications. (Wikipedia has a nice

discussion of Conway's Law, which relates difficulties in communication

specifically to corresponding flaws in software developments.

However,

certainly someone must have cited its obvious generalization to other types

of systems. Surprisingly, I don't think I've mentioned Conway's Law

previously in RISKS, although I have been referring to it explicitly and in

its generalized forms for many years. Melvin, not John.) PGN]

⚡ Another power outage brings down German TV station

<Debora Weber-Wulff <D.Weber-Wulff@fhtw-berlin.de>>

Sun, 26 Nov 2006 18:31:56 +0100

Sunday morning, Nov. 26, 2006 there was a power outage in Hamburg-Lokstedt, where the German TV station NDR has its headquarters.

This time it was Vattenfall, not EON that was responsible for the power-out.

Both the regular medium voltage and the emergency power system were knocked out. It took about 90 minutes for broadcasting to be completely resumed.

<http://www.netzeitung.de/medien/455451.html> with links to other reports

This is the second time in one week that a TV station has dropped out of the ether, last week both Hamburg 1 and ZDF were offline after a power outage in Hamburg-Rothenbaum.

NDR itself explains at http://www1.ndr.de/ndr_pages_std/0,2570,OID3392462,00.html that it was not actually a power outage. Ivo Banek, a speaker for Vattenfall, said that there were numerous short-circuits in the 50 km long cable in Lokstedt. It happened in the span of a few milliseconds, and normal electrical customers will not have noticed anything. This brought down the electricity for the TV station, however, and a ground fault brought the emergency power system to its knees.

It is still not clear what caused the shorts.

Prof. Dr. Debora Weber-Wulff, FHTW Berlin, Internationale Medieninformatik,
10313 Berlin <http://www.f4.fhtw-berlin.de/people/weberwu/> +49-30-5019-2320

The UK NHS IT plan

<Brian Randell <Brian.Randell@ncl.ac.uk>>

Tue, 5 Dec 2006 11:37:00 +0000

MPs will hold an inquiry into 12-billion-pound NHS IT plan after some MPs expressed concerns that the scheme may be foundering. The decision reverses a resolution taken by the parliamentary committee only weeks ago not to hold an inquiry, and vindicates a campaign led by leading academics.

[Source:

Tony Collins, *Computer Weekly*, 28 Nov 2006; PGN-ed]

<http://www.computerweekly.com/Articles/2006/11/28/220206/mps-will-hold-inquiry-into-12bn-nhs-it-plan.htm>

[Brian has been involved in this campaign to get an inquiry held into the

problems arising in connection with the National Health Service National

Programme for IT ("NPfIT", which strangely reminds me of Tom Lehrer's

Boston subway song punchline -- "HCKC-PW"). He is pleased to report that

they have had some success. PGN]

[Brian also reports that the public dossier (<http://nhs-it.info/>) that

he edits on this subject continues to grow. This is an extraordinarily

good analysis, and well worth reading. The RISKS-related lessons are

profound, although unfortunately not unusual. PGN]

Rebooting airplanes

<"Douglas W. Jones" <jones@cs.uiowa.edu>>

Tue, 28 Nov 2006 13:29:42 -0600

In the last few weeks, I've done quite a bit of flying, and twice, now, I've been on planes where they had to reboot.

The first trip where this happened, as we were scheduled to leave the gate, there was a delay, and then the pilot said over the intercom: "We're having trouble with some of the cockpit instruments, so I'm going to force a hard reboot by switching off all the power for a bit." The lights and all other power on the plane then went off, and after a fifteen second pause, on again. A minute later, the pilot said: "That seems to have fixed the problem," and we were off.

I wasn't impressed. As far as I am concerned, this is clear evidence of a genuine design error somewhere in the system.

The second problem happened on Sunday, on a flight back from Amsterdam. On that flight, they had serious problems with the in-flight video on demand system. They tried a "soft reboot" of some kind, and it didn't work, so they then tried two "hard reboots," their term, and after the second try, it worked fine. Their instructions were "until the system comes all the way up, please don't touch any buttons." That alone suggests poor design. The system ought to come up with interrupts disabled on any devices that it's not ready to listen to, after all.

The reboot process took close to half an hour, and watching the displays in

the seat backs that were visible from my seat, I could see that they were being rebooted in sequence, about one per second. Furthermore, as each in-seat display was rebooted, it showed the Linux penguin and then a Linux boot script, revealing that each seat-back display was a little Linux system, suggesting that they were all networked to a video server for the plane.

Again, the need for these global reboots is strong evidence that the systems were not well designed,

I wonder if both of these stories illustrate problems with the kinds of graduates we are turning out these days. CS programs across the country are emphasizing high-level courses in web programming, but fewer and fewer students know anything about the fundamentals of parallel programming that underly things. So, in constructing the kinds of distributed applications that show up in contexts like streaming video and cockpit instrumentation, they are working without the theoretical underpinnings needed to understand the problems they encounter.

✶ Mascalls, Manchester, what's the difference?

<msb@vex.net (Mark Brader)>

Sat, 2 Dec 2006 04:36:21 -0500 (EST)

A British ambulance crew, transferring a patient to a hospital where they

had never gone before, drove 200 miles out of their way before realizing that their satellite navigation device had given them the wrong directions.

These reports

<http://www.timesonline.co.uk/article/0,,2-2482605,00.html>

http://www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=419836&in_page_id=1770

mention other incidents of sat-nav gaffes, but don't say what the actual

error was this time; this shorter one

<http://www.thesun.co.uk/article/0,,2-2006551015,00.html>

says that the system showed their destination's address as being in

Brentwood in Manchester instead of Brentwood in West London.

The patient was not harmed, and the crew has been told they should have known better.

Mark Brader, Toronto, msb@vex.net

✶ Three guilty of identity fraud which netted millions

<Brian Randell <Brian.Randell@ncl.ac.uk>>

Fri, 1 Dec 2006 15:37:45 +0000

On the eve of "Black Thursday", the Russian banks' liquidity crisis of August 1995, Anton Dolgov, the head of the Moskovsky Gorodskoi Bank, disappeared leaving debts of around \$100m. Since then he had been hiding under many aliases. On 30 Nov 2006, he appeared in a London court, reportedly the head of an international identity theft gang that had defrauded thousands of account holders out of millions of pounds

over a period of 10 years, using compromised credit cards, false documents, and a bogus law firm. Dolgov pleaded guilty to four conspiracy charges.

[Source: David Pallister, 1 Dec 2006, *The Guardian* (UK); PGN-ed]

<http://www.guardian.co.uk/crime/article/0,,1961441,00.html>

School of Computing Science, Newcastle University, Newcastle upon Tyne,

NE1 7RU, UK <http://www.cs.ncl.ac.uk/~brian.randell/> +44 191 222 7923

Identity theft made easy

<John Haselsberger <jhasels99@fast.net>>

Sun, 29 Oct 2006 09:26:34 -0500

My large eastern bank abandoning the vendor servicing their Visa credit cards and bringing the task in-house. They sent out forms which we must fill out and sign in order to accept this situation. The top of the form says "For your Visa card ending in 9999". The form has out name and address and an "acceptance code" pre printed. Yet they ask for the end user to manually fill in: SSN, date of birth, mothers maiden name, and home phone, plus they want you to enter your existing (still valid) credit card number!!!! So on one small piece of paper, they create the perfect identity-theft kit, with information they already have on file. While one piece of information might be necessary for me to prove who I am to accept this offer, I am

sure their
fraud department will be busier than need be in the near future.

⚡ Federal Reserve E-Banking System Outages: Brian Krebs

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

Sun, 3 Dec 2006 09:44:18 PST

A system widely used by U.S. banks to process large volumes of payroll, credit and debit card transactions experienced intermittent outages on 27-28 Nov 2006, possibly due to some sort of malfunction or communications failure in portions of the Federal Reserve's "automated clearing house" (ACH) network, according to Security Fix -- which received an anonymous tip from an individual who claimed to work at a mid-sized bank that experienced trouble transferring ACH files across the Fed's network. [Source: Brian Krebs on Computer Security, *The Washington Post*, 28 Nov 2006; PGN-ed with thanks to Jim Horning for spotting Brian's blog, which gives further details.]
http://blog.washingtonpost.com/securityfix/2006/11/federal_reserve_ebanking_syste.html

⚡ How To Tell If Your Cell Phone Is Bugged

<Lauren Weinstein <lauren@vortex.com>>

Tue, 5 Dec 2006 12:15:54 -0800 (PST)

Greetings. A story is making the rounds right now regarding FBI use of cell phones as remote bugs (e.g. <http://news.com.com/2100-1029-6140191.html>). I originally wrote about this concept in my PRIVACY Forum in 1999 ("Cell Phones Become Instant Bugs!" - <http://www.vortex.com/privacy/priv.08.11>) so the issue is real, but we still need to bring the current saga back down to earth.

This discussion doesn't only relate to "legal" bugs but also to the use of such techniques by illegal clandestine operations, and applies to physically unmodified cell phone hardware (not phones that might have had separate, specialized bugs physically installed within them by third parties) ...

[Full article at: <http://lauren.vortex.com/archive/000202.html>]

🔥 Firefox flaw causes engagement to break off

<<Mark.Lutton@thomson.com>>

Fri, 1 Dec 2006 12:54:32 -0500

You can read the whole thing here:

https://bugzilla.mozilla.org/show_bug.cgi?id=330884

In a nutshell, the password manager can save or not save passwords for individual sites. He secretly visited many dating sites and wisely selected "don't save password." She happened to see the list of "don't save password" sites in the configuration. They are no longer

engaged.

Mark Lutton, Business Intelligence Services, a Thomson Business

🔥 Critical Firefox hole allows password theft

<Monty Solomon <monty@roscom.com>>

Tue, 28 Nov 2006 14:07:33 -0500

[http://www.computerworld.com/action/article.do?
command=viewArticleBasic&taxonomyId=17&articleId=9005379](http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyId=17&articleId=9005379)

<http://www.info-svc.com/news/11-21-2006/>

<http://secunia.com/advisories/23046>

🔥 REVIEW: "Phishing: Cutting the Identity Theft Line", Liniger/Vines

<Rob Slade <rmslade@shaw.ca>>

Fri, 01 Dec 2006 13:49:39 -0800

BKPHSHNG.RVW 20061014

"Phishing: Cutting the Identity Theft Line", Rachael Liniger/
Russell

Dean Vines, 2005, 0-7645-8498-7, U\$29.99/C\$38.99/UK#18.99

%A Rachael Liniger

%A Russell Dean Vines

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 2005

%G 0-7645-8498-7

%I John Wiley & Sons, Inc.

%O U\$29.99/C\$38.99/UK#18.99 416-236-4433 fax: 416-236-4448

%O <http://www.amazon.com/exec/obidos/ASIN/0764584987/>

robsladesinterne

<http://www.amazon.co.uk/exec/obidos/ASIN/0764584987/robladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/0764584987/robladesin03-20>

%O Audience i+ Tech 2 Writing 2 (see revfaq.htm for explanation)

%P 309 p.

%T "Phishing: Cutting the Identity Theft Line"

The introduction to the book provides a good, and very realistic, prologue to the topic of phishing. The audience for the work is said to consist of executives and incident response teams for banks and large corporations, information security professionals, and general Internet users.

Chapter one furnishes the reader with a solid overview of the subject, although it would seem to be aimed primarily at individual Web and email users. "Phishing Emails," in chapter two, explains various spam hiding and URL obfuscation technologies. The list is not exhaustive, but is sufficient to illustrate the basic concepts clearly. (The writing, in this chapter by Rachael Liniger, is delightful. Wit and humour are used extensively, and to good effect.) Chapter three presents information on false or obfuscated URLs, as well as useful detail on pop-ups: the content is much superior to other sources on the same topic. (There is also an oddly placed section on public key encryption.) Spyware is reviewed in chapter four.

You cannot stop phishing completely, notes chapter five, examining various players in the fight against identity theft and the limitations of the action they can take. Chapter six is supposed to be about helping the

organization to avoid phishing, and sets forth some policies in regard to email and Websites that are very practical in preventing abuse. (The section on authentication schemes is less so, and eventually the chapter devolves into random topics.) A generic and sometimes terse outline of incident response and network forensics makes chapter seven poor in relation to other parts of the book. In terms of consumer education, chapter eight has a number of recommendations for safer computing, with lots of "avoid Microsoft" advice, but also configuration settings, a bit of email analysis material, and an admonition to check your home finance statements carefully. Chapter nine deals with actions to take if you, personally, are the victim of identity theft. (Most of the agencies mentioned are based in the United States, but the resource list does have some additional contacts for the UK and Germany.)

Identity theft (and, by extension, phishing) is a major problem, and not enough is being done to address the issue. This book lays out the risks and threats clearly, and proposes practical solutions for a variety of actors in the drama. The text is readable and the concepts are clear. I can recommend this work to almost anyone involved in a security role, particularly those in the financial or online industries, law enforcement, or working in the field of security awareness.

copyright Robert M. Slade, 2006 BKPHSHNG.RVW 20061014
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>

REVIEW: "The Security Risk Assessment Handbook", Douglas J. Landoll

<Rob Slade <rMslade@shaw.ca>>

Wed, 15 Nov 2006 10:32:14 -0800

BKSCRAHB.RVW 20060919

"The Security Risk Assessment Handbook", Douglas J. Landoll,
2006,

0-8493-2998-1

%A Douglas J. Landoll

%C 920 Mercer Street, Windsor, ON N9A 7C2

%D 2006

%G 0-8493-2998-1

%I Auerbach Publications

%O +1-800-950-1216 auerbach@wgl.com orders@crcpress.com

%O <http://www.amazon.com/exec/obidos/ASIN/0849329981/>

[robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0849329981/robsladesinterne)

<http://www.amazon.co.uk/exec/obidos/ASIN/0849329981/>

[robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0849329981/robsladesinte-21)

%O <http://www.amazon.ca/exec/obidos/ASIN/0849329981/>

[robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0849329981/robsladesin03-20)

%O Audience a Tech 2 Writing 1 (see revfaq.htm for explanation)

%P 473 p.

%T "The Security Risk Assessment Handbook"

Chapter one is an introduction. Landoll's text is initially rather preachy and biased. The first couple of sections appear to take the position that industry has failed in its responsibility to secure information systems, and therefore (the United States federal) government has had to take charge. He then lists (although does not describe in any detail) various security

frameworks and guidelines, and argues that, simply on the basis of a lack of congruence between these documents, "best practices" are a myth. His conclusion, that risk-based security planning is better, seems oddly gleeful in the context of such an otherwise dour piece of writing.

Unfortunately, the author does not seem to do any better with risk-based security planning, right off the top. We are told (on page four) that "the establishment of an information security program is not the topic of this book. The topic of this book is how to perform and review an information security program," which statement(s) must surely rank highly in terms of self-contradiction and confusion.

Were the reader to quit after this inauspicious, muddled, and verbose beginning, however, it would be to miss a work of some value. Within pages, Landoll clarifies the rationale for, and types of, risk assessment, as well as explaining the purpose of this volume in light of other existing assessment tools and documents. (To his credit, where other authors tend to denigrate alternative references, Landoll notes their respective strengths, and then states the extension that his book provides.)

It is frustrating to attempt a single assessment of the book. The text has value, but also annoyances. Chapter two provides a useful guide to the basic components of the risk assessment process (which forms the structure for much of the rest of the book). At the same time, where Landoll has been using the business-oriented breakdown of control types (into

administrative, technical, and physical), when discussing safeguards he suddenly switches to the categories of preventive, detective, corrective, et cetera, that are more familiar to those in the government and military. (Interestingly, for someone from a strongly governmental background, Landoll does not fill out the list with recovery, compensating, deterrent, and directive.) In addition, when reviewing the concept of residual risk, two new terms of "static" and "dynamic" risk are introduced. Although the terms are poorly defined, "static" seems simply to refer to residual risk, while "dynamic" appears to mean nothing more than risk itself. Therefore, these two new entries provide no distinct value to the discourse, and only serve to confuse the issues.

Again, chapter three covers the vital topic of the definition of objectives and scope of a risk assessment project. When discussing the "customer" for a review, "Risk Assessment Method" and "Objective Review" seem to be presented as potential clients. While the question of quality of work would certainly appear to be a legitimate concern in dealing with project extent, Landoll includes a great deal of material relevant only to the final report, such as grammatical correctness and visually pleasing presentation. On the other hand, there is a good deal of very practical content addressing issues of realistic scope and reasonable budgeting. The preparation phase is covered in chapter four, dealing both with practical issues such as letters

of introduction, more esoteric concerns of system and asset criticality, and also reviewing a number of methodologies and approaches to risk assessment (although primarily at a conceptual level).

Chapter five starts a string of chapters on various types of data collection. It leads off with general discussions on the topic, examining questions of sampling and related issues. (Landoll is not always careful about explaining terms before starting to use them: neither the index nor any part of the text notes that the RIIOT method, which is used extensively in the chapter, is merely an acronym for the phases of review, interview, inspect, observe, and test.) The gathering of data on administrative safeguards, in chapter six, has good checklists of items to assess, and uses the RIIOT format to structure the areas and phases of the elements to consider. (There is a rather odd reluctance to discuss policy, and an even stranger overemphasis on two-man controls.) Moving into technical countermeasures, chapter seven starts off with a section on attacks and controls. There are very odd errors in the text: the distinction between SPAM (the Hormel food product) and spam (bulk unsolicited commercial or fraudulent messages) may be subtle but every security specialist should know it and yet Landoll uses SPAM throughout. The section on antivirus protection is weak, cross-references are spotty, and Landoll uses an old (and generally abandoned) type of firewall (session-level, which is an amalgamation of stateful and circuit-level proxy). Intriguingly, authentication is not addressed with technical controls, but

(rather weakly) with physical protection, in chapter eight. Most of the discussion of physical security outlines particular safeguards, and there is little deliberation on risk assessment or the factors that can influence it. (For example, various power supply alternatives are discussed, including the rather esoteric flywheel generator, but the idea of requesting information from the utility on past power outages doesn't seem to have occurred to the author.)

Chapter nine does turn to security risk analysis, briefly, but with some helpful pointers for the evaluation process. Risk mitigation, in chapter ten, looks rather tersely at choice of controls, and does an oddly complicated review of cost/benefit analysis. Styles for different types of reports resulting from risk assessment are outlined in chapter eleven. Chapter twelve presents a fairly standard look at project management (with extra emphasis on reporting). Chapter thirteen lists, but does not adequately describe, various risk assessment methodologies.

Despite the weaknesses, oddities, and gaps in the book, it does provide a decent overall guide, and some very useful practical suggestions. It is not quite complete in all areas, and therefore likely unsuitable as the sole source of advice on the risk assessment process for the novice, although the newcomer would not go far wrong in following the counsel of this work. The experienced security or risk assessment professional will still find valuable recommendations and advice. For anyone in the security

or risk
analysis field, the book is well worth considering.

copyright Robert M. Slade, 2006 BKSCRAHB.RVW 20060919
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<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

Search RISKS using [swish-e](#)

Volume 24: Issue 49

Sunday 10 December 2006

Contents

- [Health Hazard: Computers Spilling Your History](#)
[Milt Freudenheim and Robert Pear via Monty Solomon](#)
- [Re: Mascalls, Manchester, what's the difference?](#)
[Chris D.](#)
- [The risks of relying on Online Directions: Death?](#)
[Paul Ferguson](#)
- [Re: Yet another canceled public sector IT project](#)
[Richard Karpinski](#)
- [Trig routine risk: an oldie](#)
[Doug McIlroy](#)
- [Vulnerability in Microsoft Word Could Allow Remote Code Execution](#)
[Monty Solomon](#)
- [Risks of driving a car that uses plastic parts in critical areas](#)
[Kent Hartfield](#)
- [Research based on RISKS forum data at UBC, Canada](#)
[Hafiz Abdur Rahman](#)
- [Computers, Freedom, and Privacy, CFP 2007](#)
[Stephanie Perrin](#)

- [REVIEW: "Incident Response", E. Eugene Schultz/Russell Shumway](#)
[Rob Slade](#)
 - [REVIEW: Sarbanes-Oxley IT Compliance Using COBIT and Open Source Tools](#)
[Rob Slade](#)
 - [REVIEW: "Kim", Rudyard Kipling](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Health Hazard: Computers Spilling Your History

<Monty Solomon <monty@roscom.com>>

Sat, 2 Dec 2006 21:14:22 -0500

Bill Clinton's identity was hidden behind a false name when he went to NewYork-Presbyterian Hospital two years ago for heart surgery, but that didn't stop computer hackers, including people working at the hospital, from trying to get a peek at the electronic records of his medical charts.

The same hospital thwarted 1,500 unauthorized attempts by its own employees to look at the patient records of a famous local athlete, said J. David Liss, a vice president at NewYork-Presbyterian.

And just last September, the New York City public hospital system said that dozens of workers at one of its Brooklyn medical centers, including doctors and nurses, technicians and clerks, had improperly looked at the computerized medical records of Nixzmary Brown, a 7-year-old who prosecutors say was beaten to death by her stepfather last winter.

Powerful forces are lobbying hard for government and private

programs that could push the nation's costly and inefficient health care system into the computer age. President Bush strongly favors more use of health information technology. Health insurance and medical device companies are eager supporters, not to mention technology companies like I.B.M. and Google. Furthermore, Intel and Wal-Mart Stores have both said they intend to announce plans this week to embrace electronic health records for their employees. ...

[Source: Health Hazard: Computers Spilling Your History, by Milt Freudenheim and Robert Pear, *The New York Times*, 3 Dec 2006]

<http://www.nytimes.com/2006/12/03/business/yourmoney/03health.html?ex=1322802000&en=b2c0f7946b4e3d9d&ei=5090>

✉ Re: Mascalls, Manchester, what's the difference? (Brader, [R-24.48](#))

<"Chris D." <e767pmk@yahoo.co.uk>>
Sat, 09 Dec 2006 22:54:07 +0000

> says that the system showed their destination's address as
being in
> Brentwood in Manchester instead of Brentwood in West London.

Looks like another navigational error -- the correct destination was Brentwood, Essex, about 25 miles/40km north-east of downtown London; BrentFORD is the suburb in west London. Probably fortunate that the ambulance wasn't headed for Edmonton, north London, or they may have ended

up in Alberta! The UK has plenty of traps like this, such as St Ives, Cornwall, being about 270 miles/430km from St Ives, Cambridgeshire. Then there are Tunbridge Wells and Tonbridge, only 5 miles/8km apart but different towns, and not far from Leeds Castle, which is nowhere near the city of Leeds, Yorkshire. Of course localities may have a colloquial name not shown on maps as well.

This sort of thing makes for amusing news items, but it can have serious consequences. It reminded me of reported problems with a computer-based despatching system for ambulances in London some years ago, and a quick Google search came up with [RISKS-14.48](#), which included this item:

```
> London Ambulance Service Inquiry Report (long)
> <Brian.Randell@newcastle.ac.uk>
> a) a need for near perfect input information in an imperfect
world;
```

As I understand it, part of the problem was ambiguous or imprecise locations given for incidents; in an emergency situation, callers may just yell out the name of the nearest landmark, or their own name for an area, which may well not match the computer's database.

Also this week (7 Dec) came the story of the Kim family who were stranded on remote Bear Camp Road in Oregon, possibly after using an on-line map which did not show the road as unsuitable for winter use, unlike some other paper and on-line maps. Temptation is to blame the map compilers for inadequate warnings.

As ever, looks like the way to minimise RISKS when traveling in unfamiliar areas is to get hold of as much information as you can from different sources first, and run a sanity check before you start (what sort of distance/time/hazards are involved?).

Cheers, Chris Drewe, not far from Brentwood, Essex County, UK.

⚡ The risks of relying on Online Directions: Death?

<"Fergie" <fergdawg@netzero.net>>

Thu, 7 Dec 2006 06:56:15 GMT

This is a very, very tragic story, which perhaps could have been compounded by the possibility that the Kim family may have indeed relied upon bogus online directions in the travels in Oregon over the Thanksgiving Day holidays.

<http://fergdawg.blogspot.com/2006/12/some-disturbing-news-online-directions.html>

Thanks to Jon. O. for pointing this out.
Our hearts go out to Katie Kim and her family.

"Fergie", a.k.a. Paul Ferguson, Engineering Architecture for the Internet
fergdawg(at)netzero.net ferg's tech blog: <http://fergdawg.blogspot.com/>

⚡ Re: Yet another canceled public sector IT project (Thomas, [R-](#)

24.47)

<Richard Karpinski <dick@cfcl.com>>

Wed, 22 Nov 2006 22:04:21 -0800

> 11m pounds wasted because no-one did a decent requirements analysis?

This is one tiny aspect of a clearly major problem. The high fraction of huge IT projects which get canceled, often after the entire budget has been spent, is an outrageous failing of the entire IT industry. In fact a significant cause is our time honored approach to requirements analysis.

We expect to get the entire set of requirements fixed before the multi year contract is signed. This is absurd. One does not head from St. Louis to New Orleans on the Mississippi River by pointing the boat in the right direction and tying the rudder. Instead we make constant course corrections to stay in the navigable parts of the river.

See instead how Tom Gilb approaches such problems in his book, "Competitive Engineering".

What we should be addressing is delivering value to (all) the stakeholders. We need to determine the purposes the system is intended to serve and establish some ten or twelve critical and measurable goals. Then we engineer a general approach and find and evaluate a modest set of improvements to address those goals. Finally we pick the lowest cost, highest value phases to implement and test next. Rinse and

repeat. Each such phase should be constrained to consume at most a few percent of the project resources before it is delivered to end users (or their proxies) for testing and evaluation.

The conventional requirements analysis delivers a shopping list of more than a hundred specific functions for the system. Each function is something that someone thought was a good idea and others signed off without very much analysis and without measurable quality objectives. This results in systems where a large fraction of the required functions, typically thirty to fifty percent, never even get used. What a waste.

With the requirements all fixed in advance, there is no opportunity to accommodate the inevitable changes in the world or even to learn from the early efforts in building the system. Experienced project managers learn to control the requests for changes to the specifications by establishing committees to impede their acceptance. Such requirements changes are seen as annoyances instead of being welcomed as course corrections which will yield a more useful and valuable final system.

Gilb calls his approach evolutionary delivery, but I prefer to call it extreme incrementalism. In addition to completely eliminating these horrendous massive failures, the method even eliminates the incredible debt burden imposed by denying the users any access to the benefits of the intended system until the completion of the entire years long project. What

foolishness.

Of course, contractors with experience will claim that their project cannot be done in such tiny pieces. They are wrong, but then they see no need to change their ways since they get paid even for systems which are canceled before they are finished or worse, get completed and then abandoned.

The better incremental methods are proven by repeated successes which you can discover at gilb.com and malotaux.nl or by contacting the companies which have adopted their approach in the last thirty some years. Despite these successes, the evolutionary method is still considered radical and risky by almost everyone who has not studied under the masters who developed it and actually applied it to their own projects.

Without such radical changes to the way things are done in IT, we can guarantee that RISKS will never run out of such disaster stories.

Richard Karpinski, World Class Nitpicker 707-546-6760 dick@cfcl.com

NOTE: "nitpicker" in the subject line gets past my spam filters.

Trig routine risk: an oldie

<Doug McIlroy <doug@cs.dartmouth.edu>>

Sat, 9 Dec 2006 11:14:18 -0500

Sometime around 1961, a customer of the Bell Labs computing center questioned a value returned by the sine routine. The cause was

simple: a card had dropped out of the assembly language source. Bob Morris pinned down the exact date by checking the dutifully filed reversion tests for system builds. Each time test values of the sine routine (and the rest of the library) had been printed out. Essentially the acceptance criterion was that the printout was the right thickness; the important point was that the tests ran to conclusion, not that they gave right answers. The trouble persisted through several deployed generations of the system.

BTW, I may have committed a sin 'cos I wrote "reversion" instead of "regression", but neither word was current then -- so I seek not remission for going off on a tangent.

[This clearly needed an overseeing SineCure. Arc the hair-old angles swing. PGN]

⚡ Vulnerability in Microsoft Word Could Allow Remote Code Execution

<Monty Solomon <monty@roscom.com>>

Wed, 6 Dec 2006 08:38:11 -0500

Microsoft Security Advisory (929433), 5 Dec 2006

Microsoft is investigating a new report of limited "zero-day" attacks

using a vulnerability in Microsoft Word 2000, Microsoft Word 2002,

Microsoft Office Word 2003, Microsoft Word Viewer 2003, Microsoft Word 2004 for Mac, and Microsoft Word 2004 v. X for Mac, as well

as
Microsoft Works 2004, 2005, and 2006.

In order for this attack to be carried out, a user must first open a malicious Word file attached to an e-mail or otherwise provided to them by an attacker.

As a best practice, users should always exercise extreme caution when opening unsolicited attachments from both known and unknown sources. ...

<http://www.microsoft.com/technet/security/advisory/929433.msp>

✶ Risks of driving a car that uses plastic parts in critical areas

<"Hartfield, Kent" <kent.hartfield@lmco.com>>

Fri, 08 Dec 2006 07:55:59 -0600

I drive a 1990 Honda Accord that was purchased used 8 years ago. It's had it's share of minor failures and repairs but has overall been a great car. Yesterday, and at first unknown to me, it had a whopper of a failure.

On my way to work a little plastic doohickey that spans the gap between the brake pedal and the brake light switch disintegrated and fell to the floorboard. In normal operation the switch is open when the brake pedal presses against it through the plastic doohickey. When the brake pedal is pressed, it moves away from the switch and that movement causes the switch

to close, thus activating the brake lights.

So, unbeknownst to me (and I truly dislike being in a state of unknowing)
the brake lights were in a state of constant on. And
furthermore, deepening
my state of unknowing, the brake lights will operate when the
key is not
in the ignition. And so they did when I parked my car at my
wonderful place
of employment, as I was also in a state of inobservance and
there were no
bells in the car to ring for this particular occurrence as there
are for
unbuckled seatbelts, as well as headlight switch and key in
ignition
oversights.

At the end of the workday I was relieved of my state of
unknowing when I
approached my car and saw what I thought were tail lights
illuminated on the
car, signaling apparent stupidity to all who wandered by that
day. As I saw
the headlights were not on, my state became one of confusion and
then of
dismay as I tested the ignition and found I would have to beg a
jump from a
fellow, but smirking, engineer (as I would smirk myself, no
doubt, had the
situation been reversed).

That being done and the car being made to run, on the long ride
home I
puzzled out that it must be the brake lights that had remained
on and not
the tail lights. So now I suffer the indignity of appearing to
ride the
brakes, as though I need two feet to accomplish a chore when one
foot will
do quite nicely. When home I performed the investigation that
revealed the
defective part and immediately replaced it with a metal

doohickey of similar
design and exact function.

So a plastic piece breaks on my car and causes the battery to
run down?

Who'd a thunk of such a risk?

Kent Hartfield, Electro Optic Engineering,
Lockheed Martin Missiles and Fire Control

🚩 Research based on RISKS forum data at UBC, Canada

<"Hafiz Abdur Rahman" <rahmanha@gmail.com>>

Sat, 9 Dec 2006 05:50:48 -0800

We have conducted a study on origin of critical infrastructure failures using 12 years (1994-2005) of RISKS forum data. In this study, we tried to find the causes of critical infrastructure failures and their impacts in different dimensions, such as origin of failures, impacts of failures in spatial and temporal dimensions, their effect on public safety; and how failures propagate from one infrastructure to another. The results obtained from the analysis of real life failure cases, which happened over a considerable time span, should be interesting and useful for RISKS forum readers. Findings of this study have been documented in the following paper:

H. A. Rahman, K. Beznosov, J. R. Marti', "Identification of Sources of Failures and their Propagation in Critical Infrastructures from 12 Years of Public Failure Reports", CRIS, Third International Conference on

Critical

Infrastructures, Alexandria, VA, September 2006. This can be found from the following link:

http://www.ece.ubc.ca/~rahmanha/cris2006_CS2_paper.pdf

This paper has been selected for publication in the International Journal of Critical Infrastructures. We are presently working on the journal version. We welcome your suggestions/comments about possible improvements (focused more on theoretical aspects). Please send your comments to Hafiz Abdur Rahman <rahmanha@gmail.com> before January 15, 2007.

Hafiz Abdur Rahman, PhD Student, ECE, University of British Columbia, Canada
Room # 3085 Kaiser Building, Vancouver, B.C. Canada V6T 1Z4 1-604-822-2552

✶ Computers, Freedom, and Privacy, CFP 2007

<"Stephanie Perrin" <sperrin@privcom.gc.ca>>
Fri, 8 Dec 2006 17:50:38 -0500

The Seventeenth Computers, Freedom, and Privacy CFP 2007 will take place in Montreal CANADA, 1-4 May 2007. Proposals are due 20 Jan 2007. See the website for details:

<http://www.cfp2007.org>

[Stephanie is the Chair this year. I've been to about half of the past

CFPs, and it is usually a very thought-provoking meeting, with many

RISKS-related issues typically on the program. PGN]

REVIEW: "Incident Response", E. Eugene Schultz/Russell Shumway

<Rob Slade <rmslade@shaw.ca>>

Fri, 17 Nov 2006 15:21:49 -0800

BKIRSGHS.RVW 20060906

"Incident Response", E. Eugene Schultz/Russell Shumway, 2002,
1-57870-256-9, U\$39.99/C\$59.95/UK#30.99

%A E. Eugene Schultz

%A Russell Shumway

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

%D 2002

%G 1-57870-256-9

%I Macmillan Computer Publishing (MCP)/New Riders

%O U\$39.99/C\$59.95/UK#30.99 800-858-7674 317-581-3743 info@mcp.
com

%O [http://www.amazon.com/exec/obidos/ASIN/1578702569/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/1578702569/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/1578702569/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/1578702569/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/1578702569/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/1578702569/robsladesin03-20)

%O Audience i- Tech 2 Writing 1 (see revfaq.htm for
explanation)

%P 384 p.

%T "Incident Response: A Strategic Guide to Handling System and
Network Security Breaches"

Beyond saying that security breaches occur, and that we need to respond to them, the introduction doesn't tell us much about either the topic or the book.

Chapter one contains a good deal of material with which security professionals will agree, but it does not provide helpful

guidance. The attempt to define "incidents" is not wrong in any particular, but is tautological and of limited utility. "Risk Analysis," in chapter two, briefly repeats the usual procedures, but expends most of its text in details of specific (mostly network) system attacks. A suggested methodology for incident response is provided in chapter three, along with a justification for the use of a formal process. (Many may find it ironic that much of the rationale for formal methods has to do with expecting the unexpected.) (The process is given in the acronym PDCERF; which stands for preparation, detection, containment, eradication, recovery, and followup; but the text, rather unsettlingly, presents a number of variations on the acronym throughout the chapter.) Chapter four deals with forming and managing an incident response team, and the content is mostly concerned with communications, corporate culture, and management. This material is extended in chapter five, which covers other factors involved with organizing for incident response.

Chapter six turns to a slightly more technical topic, regarding the tracing of network attacks. This is an overview, with only limited technical content, but even so a few items are suspect (such as the implication that MAC [Media Access Control] addresses are permanent and fixed). Legal issues related to incident response are reviewed in chapter seven. Chapters eight and nine provide an overview of computer forensics, as well as good advice on the handling and management of evidence, but at a conceptual,

rather than technical, level. Insider attacks are difficult to determine and protect against, and chapter ten tacitly admits this by spending a lot of time just telling stories. Chapter eleven (written by an outside author) examines criminal profiling and other incident response factors related to social sciences. Honeypots and other types of deception aimed at the attacker are the subject of chapter twelve. Chapter thirteen finishes off with a look at emerging tools and directions.

While still flawed, this work is probably more practical than Mandia and Procise's law enforcement oriented volume (cf. BKINCDRS.RVW), van Wyk and Fornas's somewhat less detailed work (cf. BKINCRES.RVW), or Schweitzer's basic and wordy tome (cf. BKINCRSP.RVW) (all, of course, are entitled "Incident Response").

copyright Robert M. Slade, 2006 BKIRSGHS.RVW 20060906
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>

REVIEW: Sarbanes-Oxley IT Compliance Using COBIT and Open Source Tools

<Rob Slade <rMslade@shaw.ca>>
Wed, 29 Nov 2006 21:07:16 -0800

Christian B. Lahti/Roderick Peterson

BKSOITCU.RVW 20061013

"Sarbanes-Oxley IT Compliance Using COBIT and Open Source Tools",
Christian B. Lahti/Roderick Peterson, 2005, 1-59749-036-9,
U\$49.95/C\$69.95

%A Christian B. Lahti

%A Roderick Peterson

%C 800 Hingham Street, Rockland, MA 02370

%D 2005

%G 1-59749-036-9

%I Syngress Media, Inc.

%O U\$49.95/C\$69.95 781-681-5151 fax: 781-681-3585 www.syngress.com

%O <http://www.amazon.com/exec/obidos/ASIN/1597490369/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/1597490369/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/1597490369/robsladesin03-20>

%O Audience a- Tech 1 Writing 1 (see [revfaq.htm](#) for explanation)

%P 333 p. + CD-ROM

%T "Sarbanes-Oxley IT Compliance Using COBIT and Open Source Tools"

"This book is essentially a technical book, with as much applicable content as we could muster by way of open source technologies and how they fit into the Sarbanes-Oxley sphere of influence." Thus speaketh the authors in chapter one (page 4), giving us, almost immediately, fair warning that there may be problems in this book. For one thing, the Sarbanes-Oxley (SOX) law is **not** technical (if it were, the drafters would have known not to give the central point related to information technology section number 404). The authors seem to be intent on listing off all manner of open source programs, using the magic title of SOX to add legitimacy to an otherwise

aimless catalogue. (The use of vague buzzwords is also supposed to increase the perceived erudition of the work, although the authors seem to stumble occasionally, such as when they confuse the French "voila" with the musical "viola" on page 5.) If the authors were truly to answer some of the questions that they pose (for example, is open source software compliant with the law, and can it reduce the costs of achieving and monitoring compliance) then the text might have some utility. However, there is no introduction to the legislation as such, and the list of roles within an organization has little specific relevance to the issues underlying the analysis, integrity, and reporting of financial data. Most of the space in the initial chapter is devoted to screenshots of Knoppix, a poorly explained installation section, and a list of the programs in the eGroupware application.

SOX and COBIT are supposed to be defined in chapter two. SOX gets almost no exegesis, while there is a list of some of the COBIT objectives. Chapter three lists various open source security tools, has some random notes on policy and auditing, and a "sample" policy on password change. The usual promotional piece for open source software makes up chapter four, with the standard arguments for using open source, but no new rationale for the application to this particular topic.

Chapters five through eight are based on four domains from COBIT (loosely based on the Deming plan-do-check-act cycle). In sequence, we

have planning and organization, acquisition and implementation, delivery and support, and monitoring. Each of the chapters has a section entitled "What does [name of domain] mean?" but these questions are not answered in any useful way. Each chapter has an extensive (but not comprehensive) list of tasks that might be undertaken, and each delves deeply into the technical minutia of one or more isolated topics.

Chapter nine finishes off with miscellaneous advice in random areas.

If you have no experience with security, and are scared stiff of even approaching SOX, this book may get you working on some areas that will probably be useful. Mind you, if you don't get information from other sources, you may find that there are gaps in your security that you never considered. If you are experienced in security, and want to know about SOX or COBIT, and what you should do about them, you will be very disappointed with what you find in this text. If you want to know about open source security tools, you will be even more frustrated.

(Having a Knoppix boot CD around might be handy, if you know how to use it.)

copyright Robert M. Slade, 2006 BKS0ITCU.RVW 20061013
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>

REVIEW: "Kim", Rudyard Kipling

<Rob Slade <rMslade@shaw.ca>>

Fri, 08 Dec 2006 09:25:34 -0800

BKKIM.RVW 20061124

"Kim", Rudyard Kipling, 1901, 0-812-56575-4

%A Rudyard Kipling

%C 49 West 24th Street, or 175 Fifth Avenue, New York, NY
10010

%D 1901 (no, it isn't a Y2K joke)

%G 0-812-56575-4

%I Tor Books/Tom Doherty Assoc.

%O pnh@tor.com www.tor.com

%O [http://www.amazon.com/exec/obidos/ASIN/0812565754/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0812565754/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/0812565754/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0812565754/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/0812565754/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0812565754/robsladesin03-20)

%O Audience n+ Tech 3 Writing 3 (see revfaq.htm for
explanation)

%P 307 p.

%T "Kim"

Kipling packed a great deal of information and concept into his stories, and in "Kim" we find The Great Game: espionage and spying. Within the first twenty pages we have authentication by something you have, denial of service, impersonation, stealth, masquerade, role-based authorization (with ad hoc authentication by something you know), eavesdropping, and trust based on data integrity. Later on we get contingency planning against theft and cryptography with key changes.

Beyond all this, and repeatedly throughout the story, we have

social engineering: misdirection, analysis of situations and characters, the maneuvering and manipulating of people so that they do what you want, all the while thinking that it was their idea. The explanation given is at once subtle and lucid, and is both more useful and much more entertaining than that given by Mitnick in "The Art of Deception" (cf. BKARTDCP.RVW).

Kipling is, perhaps, too gentle a writer for the thriller genre. He is, though, a better wordsmith than most of those who work in that idiom. His command of dialogue is unparalleled: in "Kim" there is no need to identify the individual speakers, for they are as instantly distinguished in the text as they would be by speech.

I heartily recommend "Kim" to anyone in the security field, or anyone who wants a decent read.

copyright Robert M. Slade, 2006 BKKIM.RVW 20061124
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<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

Search RISKS using [swish-e](#)

Volume 24: Issue 50

Friday 15 December 2006

Contents

- [Florida's Voting System Certification](#)
[Rebecca Mercuri](#)
- [Midair Collision in Brasil](#)
[Peter B. Ladkin](#)
- [Don't Try to Program and Fly at the Same Time](#)
[Peter B. Ladkin](#)
- [RFID access control tokens widely open to cloning](#)
[Adam Laurie](#)
- [How Pop-Ups Could Brand You a Pervert or Crook](#)
[Lauren Weinstein](#)
- [No computer issues in Kim family navigation error](#)
[Andrew Klossner](#)
- [Time Warner Cable / Showtime Major Fubar](#)
[Simon Higgs via Dave Farber](#)
- [*The Guardian*'s billing dept. aids identity theft](#)
[Nik Clayton](#)
- [REVIEW: "Understanding and Managing Cybercrime", Samuel C. McQuade](#)
[Rob Slade](#)

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

Florida's Voting System Certification

<"R. Mercuri" <notable@mindspring.com>>

Thu, 14 Dec 2006 13:32:21 -0500

I had the opportunity to review the Florida Voting System Standards (at

<<http://election.dos.state.fl.us/laws/proposedrules/pdf/dsde101Form.pdf>>)

and have found them to be inadequate in numerous regards. My 3-page comment

on the potential inequities, inadequacies and omissions of Florida's voting

system certification process can be found at

<<http://www.notablesoftware.com/Papers/FLVSSRMComment.pdf>>

Rebecca Mercuri.

Permission granted to post and forward this e-mail message in its entirety.

Midair Collision in Brasil

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>

Wed, 13 Dec 2006 19:49:23 +0100

On 29 Sep 2006, a midair collision occurred in Brazil on Airway UZ6, between

Brasilia and Manaus, at Flight Level (FL) 370 (an altitude at an air

pressure equal to that at 37,000 ft in an International Standard Atmosphere). An Embraer Legacy business jet, on a delivery flight from the

manufacturer to a U.S. owner, apparently collided with a B737 transport aircraft, GOL Flight 1907. The GOL aircraft subsequently broke up in flight and crashed into the jungle, with the loss of all on board. The Legacy continued flying and made an emergency landing at a military airbase. New York Times columnist Joe Sharkey was on board and related the tale. (David Magda noted this accident in [RISKS-24.45.](#))

Both aircraft were equipped with Honeywell's TCAS 2000 collision-avoidance systems. It has not yet been determined why the collision avoidance systems did not issue a warning. It is suspected that the Legacy transponder, an essential component on which the TCAS is dependent, was not operating but it has not yet been determined why this would have been so. Transponders on other Embraer jets have been recently subject to an Airworthiness Directive (AD) from the U.S. FAA because of incidents in which the transponders have ceased operating during a code change without sufficient notification to the pilots, but it has been pointed out that this AD is not related to the Brazilian midair (as far as one can tell).

The flight plan of the Legacy called for an altitude of FL 360 when joining UZ6. However, the Legacy had been previously cleared to FL 370, and had subsequently lost contact with ATC, who had tried but failed to issue a descent to FL 360. US rules under such circumstances require pilots sometimes to maintain last cleared FL; sometimes to revert to flight plan, according to circumstance. I know of no source which clearly

states

Brazilian rules. The GOL aircraft was cleared on UZ6 in the opposite direction at FL 370.

The Legacy pilots have had their passports impounded and an investigation is underway to determine whether they have any criminal responsibility. Besides the human cost (they are holed up in a hotel in Rio with their lawyer and don't go outside), such a judicial process in advance of the causal investigation has been criticised by the Flight Safety Foundation, the (British) Royal Aeronautical Society, the (French) Academie Nationale de l'Air, and the Civil Air Navigation Services Organisation. FSF President Bill Voss has said "We are increasingly alarmed that the focus of governments in the wake of [civil aircraft] accidents is to conduct lengthy, expensive and highly disruptive criminal investigations in an attempt to exact punishment, instead of ensuring the free flow of information to understand what happened and why, and prevent recurrence of the tragedy" (cited in Pierre Sparaco's column A European Perspective, entitled "Unwarranted Criminalisation", in Aviation Week and Space Technology, 13 Nov 2006, p43. Sparaco has addressed this issue three times this year, the first two on 22 May 2006, p45 and 3 Jul 2006, p42, in the wake of the Concorde accident, and the fourteen-year-old Mont St.-Odile accident, which only this year came to court: the defendants were acquitted.) Similar jurisdiction conflicts arise in Germany, with investigations into accidents on the railways, and have been most recently pointed out in

consequence of
the Maglev accident (Weber-Wulf, [RISKS-24.45](#); Weber-Wulf,
Virtel, Ladkin,
[RISKS-24.44](#)).

But the computer-risk connection is this time not with TCAS.

David Kaminski-Morrow reported in Flight International, 5-11 Dec
2006, p15,
that the Cindacta-1 display software running at the ATC center
controlling
the flights can automatically update altitude-clearance
information without
controller intervention. As the Legacy joined UZ6, the system
automatically
updated the Legacy's cleared flight level to FL 360. "Loss of
the Legacy's
transponder information [which includes the actual FL] shortly
afterwards
... eliminated a crucial indication to controllers that there
was a mismatch
over its altitude." In other words, the Legacy was flying at FL
370 and the
controller's display was showing FL 360.

I omit the justified criticism from the Brazilian arm of the
International
Federation of Air Traffic Controllers' Associations, which
visited the
Cindacta-1 center and discovered this, um, feature of the SW,
because I am
sure that RISKS readers can supply their own, similar, reactions.

Peter B. Ladkin, Causalis Limited and University of Bielefeld
www.causalis.com www.rvs.uni-bielefeld.de

⚡ Don't Try to Program and Fly at the Same Time

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>

Wed, 13 Dec 2006 19:55:39 +0100

David Learmount reports in Flight International, 12-18 Dec, p16, on a Ryanair B737-800 which almost flew into terrain on 23 Mar 2006, on approach to Knock airport, Ireland. The Irish Air Accident Investigation Unit (AAIU) determined the principal cause to be that the "pilots fixated on reprogramming the flight management computer (FMC) while the aircraft continued its descent". A contributory cause was reported to be a "systemic failure" at the airline and the chart supplier Jeppesen (owned by Boeing) that failed to supply the pilots with up-to-date information about the navigation aids available at Knock.

Peter B. Ladkin, Causalis Limited and University of Bielefeld
www.causalis.com www.rvs.uni-bielefeld.de

RFID access control tokens widely open to cloning

<Adam Laurie <adam.laurie@thebunker.net>>

Mon, 11 Dec 2006 17:57:55 +0000

Too many systems to itemize here rely on the 'unique ID' of an RFID token to grant access to a system or building, and, in the case that these tokens are based on 125kHz or 134.2kHz standard tags, many of them may be vulnerable to relatively simple cloning attacks.

In a way this is nothing new - several researchers have previously presented

attacks whereby RFID tags were emulated by custom built circuits which were able to fool readers into thinking that a genuine tag had been presented.

However, the industry response was normally that this was not a 'real' threat, as it required specialist knowledge and equipment, and the resulting device was not a 'true clone' as it didn't have the same form factor as the original.

The difference here is that the 'clone' may actually follow the same form factor as the original, and is therefore indistinguishable not just to the reader, but also to the human eye. In addition, no specialist equipment or custom circuitry is required, and the 'clones' can be produced using off the shelf equipment, software and blank tags purchased perfectly legally over the Internet. In fact, the tags are only doing what they were designed to do in the first place: implement industry standards.

The problem is that many security system suppliers are integrating industry standard tag readers, and promoting the 'uniqueness' of the tag ID as a guaranteed certainty when it isn't, and thereby compromising the security of the entire system.

The two specific tag types I've looked at are:

- * Trovan 'Unique', aka EM4x02
- * FDX-B, aka EM4x05 - ISO-11784/5 (animal tags)

The description of the 'Unique' tag, from the Trovan website is as follows:

"The TROVAN UNIQUE (c) Read-Only System is well-suited to

applications that require a high level of data security. Unlike other vendors' factory preprogrammed lines, the protocol of the TROVAN UNIQUE (c) line is patented, providing unmatched protection against unauthorised third-party cloning. Each transponder is programmed with a unique 10-digit ID code during manufacture. Comprehensive automatic test methods ensure that no code exists in duplicate in any of the TROVAN UNIQUE (c) transponder types, and that codes are programmed correctly in a readable manner. Once the code is programmed at the time of the transponder's manufacture, it cannot be counterfeited or tampered with. A total of 550 billion unique ID codes is available."

Q5 are general purpose, multi-standard tags, that are capable of emulating other devices. I found that it was a standard feature of the Q5 chip to emulate a 'Unique' tag, and it was trivial to program a duplicate ID into one. The resulting tags were tested against three different systems that I have access to, and all three systems were unable to distinguish between the original and the 'clone'.

In response to my questioning the security of the Unique tags, the response I got from Trovan was: "There are a variety of H4102 versions, some of which can be emulated by a Q5 tag. Our tags are a custom version of the H4100 tag."

It should be noted that I am not pointing the finger at Trovan devices here, but the 'Unique' standard some of their tags implement and which

are generally available as a generic tag type - it is sometimes hard to tell exactly who's devices or tags are used in a specific installation, but suffice it to say that I have found 3rd party systems (one at a very recent security systems show in London) that were vulnerable to EM4x02 style cloning. The equipment required to do this was a laptop and off the shelf RFID reader/writer, but it could just as easily have been a small handheld, and so a credible threat exists of simply swiping an access tag ID in a 'walk-by' of someone leaving a building, and then producing a clone which will give full access.

I am also able to produce what seem to be accurate clones of FDX-B tags (such as the one in my dog), and also VeriChip tags, in as much as a standard FDX-B reader such as you might find at your local vet will not be able to tell the difference. I have not been able to test if a genuine VeriGuard system would also be fooled, but VeriCorp's response when I took it up with them was:

"You can take a write-once and re-writable chip and put the VeriGuard ID number on this chip, and a lot of readers will read the ID and including the VeriGuard reader. I can not tell you every but their three things that tell are unit that it is a VeriChip 16 digits not 15, timing and one other thing. We call it copying not cloning because the can't get all the information need to send to the VeriGuard reader at the right time." [sic]

The latest release of the open source python library, RFIDIOT (v0.1h), contains tools for programming both EM4x02 and EM4x05 tag IDs to Q5 or Hitag2 tags, and I would suggest that if you own (or supply) systems based on either of these standards, that you use them to audit for this vulnerability.

Full details at <http://rfidiot.org>

Adam Laurie, The Bunker Secure Hosting Ltd., Ash Radar Station, Marshborough Road, Sandwich Kent CT13 0PL UK +44 (0) 1304 814800 <http://www.thebunker.net>

⚡ How Pop-Ups Could Brand You a Pervert or Crook

<Lauren Weinstein <lauren@vortex.com>>
Mon, 11 Dec 2006 16:00:18 -0800

How Pop-Ups Could Brand You a Pervert or Crook
<http://lauren.vortex.com/archive/000203.html>

Greetings. An article in *The New York Times* today explores the problem of Web-based "pop-up" ads being used to artificially inflate Web traffic.

<http://www.nytimes.com/2006/12/11/technology/11push.html>

I'd like to point out a potentially much more serious problem related to pop-ups that can access arbitrary Web sites -- they could be used for purposes that could get innocent Web users into major legal problems.

The issue of sites triggering unsolicited access to other sites is not new.

In an IP message over a year ago ("Google's new feature creates another user

privacy problem" --

<http://lists.elistx.com/archives/interesting-people/200506/msg00190.html>),

I discussed how Google's triggering of top item "prefetch" in returned

search results could result in Firefox browsers visiting the referenced site

-- and collecting any associated cookies -- without users' knowledge (I also

suggested ways to prevent this behavior).

The essential problem is that Web logs that record users' access to sites

would record such visits as if they had been voluntarily initiated by those

users. If those destinations happen to be sites with various forms of

"illicit" materials that could be the subject of government or other

investigations that would go digging through associated access logs...

Well, you can imagine the possible complications.

Google's prefetch behavior is an example of a well-intended feature with

unfortunate negative side-effects.

On the other hand, the sorts of nefarious pop-ups described in the NYT piece

have much greater potential for intentionally serious sorts of damage, since

they can be far more flexible and directed than simple Web prefetches, and

so could put innocent consumers at even greater risk. They might not only

access pages that could get people arrested (perhaps c-porn?), but also

download files that could trigger RIAA and/or MPAA "automatic" lawsuits, or

any number of other nightmare scenarios.

It's fair to ask why anyone might want to set loose such technical monsters on innocent victims. The simple answer is that there are quite a few people out there who just want to score a point -- to prove that they can do it -- plus of course the sick minds who enjoy watching other people suffer.

If nothing else, this specter is yet another reason to block all pop-ups routinely and to disable browser prefetch as appropriate. Most of all it is a reminder to authorities that just because particular entries are present in subpoenaed Web logs, does not necessarily mean that they are accurate representations of user intent. In many cases you may actually be looking at victims, not perpetrators.

Lauren Weinstein lauren@vortex.com or lauren@pfir.org +1 (818) 225-2800

<http://www.pfir.org/lauren> <http://lauren.vortex.com> <http://daythink.vortex.com>

⚡ No computer issues in Kim family navigation error

<Andrew Klossner <andrew@cesa.opbu.xerox.com>>

Mon, 11 Dec 2006 09:55:08 -0800

The Kim family were not misled by computerized navigation. They fell off their plotted route when they missed an exit on I-5, then tried to reroute using paper maps. The fatal error was that they

mistakenly

turned onto a road whose gate had been closed and locked for the winter but which had been broken open by vandals.

[Perry Clarke had a similar take. PGN]

⚡ Time Warner Cable / Showtime Major Fubar [From Dave Farber's IP]

<Simon Higgs <simon@higgs.com>>

Thu, 14 Dec 2006 15:48:51 -0800

Time Warner Cable are mailing out Christmas cards to their customers with an offer for a free DVD promoting the Showtime cable channel.

The instructions are simple. Customers visit a web page provided with the Christmas card and enter their phone number associated with their account. There's also a privacy notice on the resulting web page that says:

"Privacy notice: Time Warner Cable respects the relationship we have with our subscribers. We will never sell or disclose your personal account information or e-mail address."

After entering their phone number, customers then receive a confirmation page with their name, address and telephone number printed on it.

You guessed it. Anyone who knows the location of the Showtime offer can go fishing for Time Warner Cable customer names, addresses and telephone numbers just by entering random phone numbers.

***The Guardian*'s billing dept. aids identity theft**

<Nik Clayton <nik@ngo.org.uk>>

Thu, 14 Dec 2006 21:45:47 +0000

This is a repost from my blog:

<http://jc.ngo.org.uk/blog/2006/12/14/identify-theft/>

I've just discovered that I've been an unwitting participant in an identify theft.

But not, perhaps, in the way that you might imagine.

Some of my writing recently made it into *The Guardian*. As is the way of these things *The Guardian* like to pay their writers, so I sent off my details to their billing department and waited for the money to come rolling in (as you do).

It turns out that, by an odd coincidence, I'm not the only Nik Clayton to write for *The Guardian*. I'm not even the first. This other Nick Clayton (note the extra c) has written a number of columns for them, and they're also about technology matters.

This much became apparent when I received an e-mail from *The Guardian*'s billing department today confirming that they had dispatched payment for two articles that Nick had written to me. This e-mail contained Nick's name and address details, and the payment details (amounts) for the articles he's

written. But it also contains my bank details (account number and sort code). The money hasn't been deposited in to my account yet, but I imagine it soon will be.

A bit of Googling turned up Nick's site, and a bit more Googling turned up a phone number, so I've called him, and had the slightly surreal experience of:

NC: Good evening. Could I speak to Nick Clayton?

TG: Speaking

NC: Hi. It's Nik Clayton here!

Now I know how Dave Gorman must feel.

I've tried calling The Guardian's billing department but the number given in the e-mail redirects to voice mail at the moment, so I'll be in touch with them again tomorrow morning.

There are at least four risks here.

First, The Guardian's billing department will apparently change the sort code, bank account, and e-mail address details that they hold for writers on the basis of a single unauthenticated e-mail. My message to them was:

Charles Arthur asked me to send my payment details for <http://technology.guardian.co.uk/online/insideit/story/0,,1954392,00.html> to you.

Sort code is ZZ ZZ ZZ, the account number is ZZZZZZZZ.

Please let me know if there are any problems.

Second, when they pay their writers they send out an e-mail that contains, in clear, the writer's name, reference number, full address, sort code, bank account number, and the values of the payments. This may well be enough to carry out a social engineering attack.

Third, this could easily have gone the other way, and my bank account details could have been forwarded to Nick Clayton. Had he been nefarious I imagine that (given that we share the same name) these could have been used to carry out a very effective identity theft.

Fourth, had I not been quite so honest I could probably have got away with this for some time --- at the very least, continuing to earn interest on the money that The Guardian have paid.

Hmm. I wonder if The Guardian would like to use this as the basis for an article.

REVIEW: "Understanding and Managing Cybercrime", Samuel C. McQuade

<Rob Slade <rMslade@shaw.ca>>
Mon, 11 Dec 2006 12:08:15 -0800

BKUMCBCR.RVW 20061105

"Understanding and Managing Cybercrime", Samuel C. McQuade, 2006,
0-205-43973-X
%A Samuel C. McQuade scmcms@rit.edu

%C 75 Arlington Street, Boston, MA 02116
%D 2006
%G 0-205-43973-X
%I Allyn and Bacon (Pearson)
%O U\$60.80/C\$77.200 www.ablongman.com
%O [http://www.amazon.com/exec/obidos/ASIN/020543973X/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/020543973X/robsladesinterne)
[http://www.amazon.co.uk/exec/obidos/ASIN/020543973X/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/020543973X/robsladesinte-21)
%O [http://www.amazon.ca/exec/obidos/ASIN/020543973X/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/020543973X/robsladesin03-20)
%O Audience i+ Tech 1 Writing 2 (see revfaq.htm for
explanation)
%P 500 p.
%T "Understanding and Managing Cybercrime"

The preface states that this book should be considered an introductory text to the field of cybercrime (although it does not define what that topic is until chapter one of the book). The guide is addressed to two audiences of students, those in the field of information technology administration and management, and those in the field of criminology. McQuade suggests that the work can be used as a primer in basic courses expounding on information systems security, and may also be used as a supporting volume for curricula in sociology, law, public administration, public policy, or ethics courses that deal with information system crime and abuse. In the Foreword, Charles Wellford notes the increase in significance of crimes related to, or perpetrated via the use of, computers. Whereas crime statistics of traditional types have been falling in recent years, cybercrime has exploded in an environment where traditional law enforcement has been largely

unprepared.

Part one introduces the field, and outlines the growth, of cybercrime.

Chapter one starts out with a valuable addition to the discussion of the sociology of cybercrime: the concept of "relative" normality and deviance of behaviour in a new and rapidly changing field. The author then moves on to note the range of terms and activities covered under the cybercrime reference, and to note the importance of defining those terms not only in regard to research, but particularly in relation to law and prosecution.

(Sam, since I have attacked the whole *concept* of salami scams for years, and have received only a single [and minimal: the "drive-through" incident noted in the RISKS-FORUM Digest] instance of one occurring, you can*not*

expect me to let footnote 11 pass unchallenged: it should be a documented citation, not a mere explanation.) The questions provided at the end of the chapter are not simply reading checks, but thoughtful items to prompt discussion of critical concepts. The protection of information and other assets is covered in chapter two, starting with the nature of information itself, moving through the standard concepts of information security, and ending up with critical infrastructure protection (which may be a bit of overkill). Chapter three reviews the various types of cyber attacks and crimes. I was intrigued to note the inclusion of a section on academic computer abuses (generally a neglected topic), and pleased with the realistic assessment of cyberterrorism, but the structure and

taxonomy of attacks could use some work. In addition, the material on malware is quite weak: the definitions for differing types are better than many in general security works, but many of the surrounding explanations are false or misleading. For example, McQuade partially uses the Cohenesque definition that viruses must infect existing programs (which is no longer true of recent versions), and implies that a user is required for viral reproduction and spread (viruses generally require some user action for invocation, but spread is usually automated). Additionally, he makes the rather questionable assertion that the skills necessary for creating malware are the same as those required to defend national security. The psychology of cybercriminals and abusers is reviewed in chapter four, which also provides a very detailed classification for social engineering, and Donn Parker's SKRAM (skill, knowledge, resources, access, motivation) model for assessing attackers. McQuade notes the difficulty in getting agreement on a profile for computer abusers, but does not address the changing style of attacks and attackers over time.

It is interesting that chapter four is not contained within part two, which addresses social thought on cybercrime. Chapter five, in a sense, extends chapter four's discussion of categories of criminals by providing an overview of major criminologic theories: it would have been interesting to see the classification schema analyzed in light of the hypotheses, but simply having the philosophies outlined here is a major

contribution to the information security literature. In assessing the impact of cybercrime, in chapter six, McQuade notes that there is both economic and social damage to be determined. However, this merely exacerbates an existing problem: the author also points out the lack of reliable information, even in regard to economic losses alone. It is difficult to know what to make of chapter seven. Titularly it promises emerging and controversial topics in cybercrime. However, the discussion of the necessity for attack skills in regard to defence (promised in chapter three) never appears. The topics that are presented would seem to extend either the first section of chapter one (noting that computers are changing various activities in society), or chapter three (listing different types of attacks).

Part three moves to the management of cybercrime: prevention and protection. Although chapter eight deals with legal philosophies and types of laws, most of the material is only relevant to the United States. The limitations on investigators, which is the primary content of chapter nine, is again mostly restricted to the United States. There is material on investigation and computer forensics (although network and software forensics do not appear to be covered), but it is fairly brief. Chapter ten's review of information security is oddly disjointed: parts are academic in tone, parts read like a "secure your home computer" pamphlet, and parts promote risk assessment models best suited to major corporations. Future activities (mostly at the

federal government level) that might help reduce cybercrime is one part of chapter eleven, the other is a discussion of computer ethics.

The book is readable, and entertaining in sections. Most of the information is reasonable. However, suggesting this as a sole text for an information security course would be unwise: it is weak in a number of technical areas.

As an adjunct text it would be excellent: the law enforcement perspective is all too often neglected in security literature.

copyright Robert M. Slade, 2006 BKUMCBCR.RVW 20061105

rslade@vcn.bc.ca slade@victoria.tc.ca

rslade@computercrime.org

<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

Search RISKS using [swish-e](#)

Volume 24: Issue 51

Friday 15 December 2006

Contents

- [Bloomington bank night depositors victims of old fashioned fishing](#)
[David Zawislak](#)
 - [Trig error checking](#)
[Martin Ewing](#)
 - [Re: A380 delivery delays](#)
[Peter B. Ladkin](#)
 - [Re: Flat train wheels](#)
[Peter B. Ladkin](#)
 - [Re: Yet another canceled public sector IT project](#)
[Gary Hinson](#) [Richard Karpinski](#) [Jack Ganssle](#) [Rex Black](#) [Richard Karpinski](#)
 - [Re: Slade on "Kim"](#)
[Michael Bacon](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Bloomington bank night depositors victims of old fashioned fishing

<David Zawislak <davidzawislak@redmail.com>>

Sun, 10 Dec 2006 18:04:27 -0600

The Bloomington, Indiana Fifth Third Bank, learned that the Internet is not the only way to be a fishing victim. Up to 11 depositors who used the night deposit slot had their deposits fished out of the slot, after one of the slot's metal security pieces had been sheared off and the bags fished out.

<<http://www.theindychannel.com/news/10473879/detail.html>>

[The article notes that a dowel rod was found next to the broken metal piece, with fishing line and a fish hook attached. No bait was required.

No switch either. No need to spare the rod. No reel-time problems. No

social engineering. Just a straightforward low-tech approach. It reminds

us of the futility of believing in high-tech solutions that can be so

easily bypassed. PGN]

⚡ Trig error checking (Re: McIlroy, [RISKS-24.49](#))

<Martin Ewing <m.ewing@snet.net>>

Sun, 10 Dec 2006 15:27:13 -0500

Doug McIlroy's report of the effect of missing punched cards on trig accuracy ([RISKS-29.49](#)) brought to mind another troubling trig episode. In the early 1990's, we were heavy into scientific calculations on the Digital

VAX-11/780 -- ephemerides which required every last drop of precision.

Sometimes the answers weren't checking out. Eventually we found that our

VAX floating point unit (a very large circuit board) was malfunctioning. It

gave slightly wrong results, but quietly - there were no system error

reports. The diagnostic was that $\sin^{**2} + \cos^{**2}$ was intermittently not

quite equal to 1 for various arguments. [NOTE: This is a positive example

of circular reasoning! PGN]

Field service got us new boards, but how could we have confidence this bug

was not recurring? In the end we ran a background routine that checked

$\sin^{**2} + \cos^{**2}$ forever. (Today, we would make it a screensaver program.)

There is a RISKS issue -- how do you know your CPU is giving good results?

There aren't any check bits for trig functions.

(Alluded to in [RISKS-16.68](#).)

🔥 Re: A380 delivery delays (Ladkin, [RISKS-24.45](#))

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>

Wed, 13 Dec 2006 18:56:06 +0100

In [RISKS-24.45](#), I reported that Bloomberg News and AEC News were saying that

Hamburg was working with CATIA Version 4 CAD-CAM SW, and

Toulouse with CATIA

Version 5.

Now comes a different story.

Nicola Clark wrote an extensive article on the A380 delivery problems in the *International Herald Tribune* this week, in which she states that the Hamburg design SW was in fact made by a U.S. company, Computervision, and dated from the 1980s. If this is so, it isn't simply a file-format problem, as one could suppose with different versions of the same SW.

The article is available at
www.iht.com/articles/2006/12/11/business/airbus.php

Peter B. Ladkin, Causalis Limited and University of Bielefeld
www.causalis.com www.rvs.uni-bielefeld.de

✉ **Re: Flat train wheels (PGN, [RISKS-24.47](#))**

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>
Wed, 13 Dec 2006 18:42:45 +0100

In [RISKS-24.47](#), PGN reported on trainset availability problems in NY/NJ, resulting from maintenance backups in replacing/retruing wheels which had flattened. In Fall, in areas with deciduous trees, a slippery film deriving from mulched fallen leaves can build up on rails. When trains accelerate or brake on rails with such a film, adhesion is much reduced and wheels can slip. The wheel tires (most trains have steel tires on wheels) can develop flat spots through rubbing at places where a slipping wheel comes to a patch with good adhesion and the speed of the wheel does not match the

train speed
over the rail. It is also not so good for the rails, but they
are less
affected.

This problem is as old as railways. What is new is the computer
dimension.

In Fall 2003, the German Railways (Deutsche Bahn, DB) had
problems with its
new electrical multiple units (EMUs, as they are called in
England; I use
the word "trainsets" henceforth), which have designators ET 423
- 426
depending on their use. The ET 425 series trainsets for regional
trains in
the Ruhr valley and eastwards through Bielefeld to Minden and
Ostwestfalen-Lippe were having serious problems of two sorts.
First, ET 425
units, which under dry conditions have extremely good braking
characteristics, were overshooting their allowable braking
distances in
slippery conditions. Since signalling, allowable line speeds,
and operations
in general depend upon trains being able to stop within a
specified braking
distance (defined by a braking performance curve), this
presented a safety
issue. Various incidents had trains passing their stopping point
by some
hundreds of meters; clearly unacceptable. Second, train
wheelsets were
developing flat spots at a much higher rate than anticipated and
there were
not enough replacement sets on hand to be able to keep the
required number
of trainsets in service.

The result was chaos in commuter and regional train service. The
trainsets
were restricted to maximum speeds of 80 kilometers per hour
(kph), half that
to which they are certified. They could not maintain the

timetable at these slower speeds, and certain trains traveling longer distances had to be turned into two trains at a suitable breakpoint: the second train departed the breakpoint at the timetabled time, with the first train arriving later at the breakpoint, leaving travelers who previously traveled on one train through that point on their journey then to take two: the first one to the breakpoint, arriving late, and a second, later, one from the midpoint onwards, causing a large increase in journey time for these unfortunate and unhappy people. And the Ruhr is the largest urban conglomeration in Germany, so there were lots of them.

Some of the trains serviced with ET 425 trainsets were replaced with locomotive-hauled sets, which with their heavier carriages were less susceptible to the problem, and could travel at their posted speeds even in the lower-adhesion conditions.

In 2004, the DB planned the trainset replacement on the most heavily affected lines in Fall from the outset, and delays were much reduced, although travelers were not as happy as they would have been with the originally-offered service.

I discussed the issues extensively in early 2004 with the railway engineer Oliver Lemke at the Institute for Railway Engineering and Traffic Safety at the Technical University of Braunschweig, and again in early 2005, and Fall 2005. The information below specifically on the ET 425 problem comes mainly

from Oliver and from the technical article "Neue Erkenntnisse zum Gleitschutzverhalten elektrischer Triebzüge" (translated: "New Findings on the Antislip Behavior of Electric Trainsets") by K.-R. Hase, S. Müther and P. Spiess, in the Eisenbahntechnische Rundschau volume 54, pp 599-610, October 2005, available online at www.eurailpress.com/archiv/artikel.php?id=8339 (I would translate the journal name as: "Railway Technical Review", but that is the name of a different journal, in English, from the same publisher.)

First, a word about brakes. There are roughly four different kinds of braking systems in common use on railways. Two of them, friction brakes and regenerative braking, brake the wheels: the first through friction (as in cars and bicycles), the second turns the motor into a generator and thereby the kinetic energy of the train into electricity (and also some heat) which is fed back into the overhead line. On trains which are certified to travel at over 160 kph, brakes acting directly on the rails are required. There are generally two kinds. Eddy-current brakes consist of electromagnets which hover some millimeters above the rail. The moving electromagnet produces an eddy current in the rail, which produces a force on the electromagnet, and thereby on the trainset to which it is attached, in the opposite direction to that of travel. Eddy-current brakes are used on very-high-speed trains to brake from high speeds, and they are relatively ineffective at lower speeds. The kinetic energy is dissipated largely as heat, and some applications have been said to have set the rails glowing. (I understand that eddy-

current

braking is also being investigated for road trucks.) Second, there are magnetic rail brakes, which are also electromagnets, but use the magnetic attraction to set themselves firmly on the rail and achieve their braking effect through friction (which also generates heat, of course).

The ET 425 units are light, and depend for various reasons more on regenerative braking than other units. For technical reasons, it is harder under regenerative braking to start a halted and sliding wheel rolling again. The ET 425 series was not certified to travel at higher than 160 kph, so did not require rail brakes. Magnetic rail brakes would have solved the braking underperformance problem directly, but the bogies (the chassis which holds the wheel sets, including the wheel sets. In the U. S. they are called "trucks") were not designed to be able to take them. Outfitting the ET 425s with magnetic rail brakes would have entailed replacing bogies, at great cost. (Back in 2005, when I was discussing this, there was a picture of a magnetic rail brake on an ET 425 on the WWW, but it is no longer there.)

There was also discovered to be an issue with the sanding devices. These spray sand just in front of the rail-wheel adhesion point to increase adhesion in conditions of low adhesion. The aerodynamics weren't quite right and at high speeds the sand was ending up elsewhere than at the point of adhesion.

The braking on the ET 425 trainsets is computer-controlled: brake-by-wire. The driver issues a braking command which consists in a target braking value (in German, "Soll"-Wert), and the computer controller figures out how to attain that value. It turns out that the braking problems were largely solved by optimising the braking algorithms implemented in the control SW. The SW was doing what it should have been doing but the algorithms for braking under non-optimal conditions of friction were not as good as they could have been.

I leave it to readers to decide whether this a computer-related problem or rather a computer-related solution to a problem. I suspect the characterisation is a matter of taste.

Mark Brader reported a problem in [RISKS-23.63](#) with braking systems on Virgin Trains's then-new Pendolino tilt-trains for the British West Coast Line, a year after the DB problems first surfaced. The BBC carried reports dated 11 November 2004 at news.bbc.co.uk/1/hi/uk/4002257.stm Brader's RISKS report referred only to the very-low-speed braking issues, because these were caused by out-of-spec SW issues, but such issues had little to do with the speed limit of 110 mph to which the BBC article also referred. It turns out that the Pendolinos also had problems with braking during leaf-mulch conditions and, unlike DB high-speed units, were neither required to be fitted with magnetic rail brakes, nor were they so fitted. (I no longer have a suitable reference for this.)

Peter B. Ladkin, Causalis Limited and University of Bielefeld

Re: Yet another canceled public sector IT project ([R-24.49](#))

<"Gary Hinson" <Gary@isect.com>>

Mon, 11 Dec 2006 11:55:09 +1300

Richard has picked out just one of many important issues that commonly affect software development projects, perhaps implying that if only this one issue were addressed, everything would be fine. If so, that's silver bullet thinking. The Real World(TM) is far more complex, for examples:

* Small projects are less risky than large ones since they are more predictable and controllable. It is sound advice to split huge monolithic projects into phases and/or to treat them as programmes containing multiple sub-projects that are, as far as possible, mutually independent. Unfortunately, some systems (such as national health systems) are inherently huge and complex, and are extremely difficult to subdivide. There are also additional costs to subdividing projects. Programme management is a more abstract, specialist and hence expensive form of project management (qualified and successful programme managers are in high demand). There are always residual dependencies between sub-projects meaning additional planning and execution risks;

* Large projects invariably involve politics, whether national or corporate/internal. There are numerous vested interests,

differing aims and competing priorities. This is a given. Dealing effectively with the politics is more art than science;

* Richard identified changing requirements specifications, fair enough.

Many other aspects of projects often change too, such is the nature of project risk and planning. It makes sense for management to anticipate the likelihood of changes and put in place, in advance: (a) contingency arrangements; and (b) the project governance structures to work proactively with whatever crops up rather than reactively picking up the pieces; and yet there is a curious faith in pre-cast plans, budgets and teams. I am fond of the concept of constantly revising the business case for major projects as they proceed from concept to delivery since the initial case prepared for budgeting purposes is highly unlikely to reflect fully the 'as built' system, both in terms of the costs and the benefits. A useful side-effect is that from the highly refined business case emerges a comprehensive blueprint for metrics to measure and maximize the value obtained from the delivered system (read John Thorp's "The Information Paradox" for more);

* Projects are themselves change activities, introducing the thorny topic of change management. We persist in referring to "software development projects" etc. rather than "organizational change initiatives" etc. The organization is of course going to be different post-implementation, significantly different in the case of large systems. Managing

the transition from pre- through para- to post-implementation is no easy task but seldom (in my experience) is it truly recognized by management as an important and difficult activity, at least until things are already going seriously wrong. The more organizational and political layers there are between developers and users, the harder it is to ensure that the project sponsor's change vision is both appropriate/feasible and reflected on the ground;

* There will always be conflicting priorities for senior management's attention. If there were not, there would be a greater risk of management 'going native' on the project, perhaps losing sight of the true business objectives and changes in the environment. On top of that, we all have different skills and motivations. The more people are involved in a project, the more diversity of views and opinions there will be.

It seems to me that management by and large needs to be more creative, professional and flexible with respect to the governance of large projects. Why not, for instance, initiate multiple parallel project teams in friendly competition to develop the best business case and project plans? Management can monitor their progress, seed good ideas between the teams and when appropriate kill off the weakest to focus resources on the most promising (my hero Charles Darwin coined the term 'survival of the fittest'). Sure there would be higher costs up front but the risk mitigation and competitive

motivation may more than compensate. 'Extreme programming' techniques, object orientation, formal methods, outsourcing etc. all potentially have their place in a creative organization that is prepared to experiment and learn. Traditional stick-in-the-mud management teams are destined to repeat the same failures over and over, and perhaps worse to stall vital projects because of the fear of failure (the risk of not doing what's necessary).

Leaning brings me to my final point. Every project, good and bad, is a worthwhile learning opportunity. Those directly involved clearly learn from the experience (subject to the limitations of their own perspectives) but it is probably worthwhile spreading the knowledge further afield. Internal Audit has a valuable role both to review and advise on the political, risk and project management during the project and to tease out and share the lessons to be learnt afterwards. Doing this repeatedly improves Internal Audit's competence and expertise.

Dr Gary Hinson PhD MBA CISSP CISM CISA, CEO IsecT Ltd. +64 634 22922

www.NoticeBored.com www.IsecT.com www.ISO27001security.com

⚡ Re: Yet another canceled public sector IT project ([R-24.49](#))

<Richard Karpinski <dick@cfcl.com>>

Sun, 10 Dec 2006 17:15:33 -0800

Gary, If it were one issue, it wouldn't have taken Gilb 474 pages to address the rather broad topic of project management. Would you like to see the PDF to understand how thoroughly he approaches the problems? I just tried to say the essential parts in a short enough form that people could read it through. It was brief.

How can you do it with extreme incrementalism and not know you are failing before you have spent ten percent of the budget? I boldly claim that you cannot. I further claim that that fact justifies my claim that the horrors of the current methods can be reliably averted by adopting extreme incrementalism.

Ask Gilb or Malotaux about their experience with it.

P.S. In fact, here is what Niels Malotaux said in response to my item:

Nice to hear from you. And all true. Every time a project gets in trouble, I ask myself: "Why didn't they just ask for a bit of help?" It's SO easy to get a project on track and let it conclude successfully, that it must be either ignorance (which it mostly is) or lack of interest (which it mostly seems to be) when people let projects fail again and again.

You say: "... evolutionary method is still considered radical and risky". I regularly get the comment that what I say is "highly controversial and philosophical". Still, we know from practice that it is highly practical and successful. Recently I saw again two

project

managers very reluctant to start letting me help getting their failing

projects on track. Only because their boss gave them the choice to either

from now on pass every milestone on time themselves (which they have never

done before), or to let me help them, they reluctantly conceded to let me

help them. Within one week, just only applying the TaskCycle, they were

convinced that this was great and helping them immensely to be more

successful. So I was thinking: "Why can't I explain people convincingly

about the Evo benefits before starting?". I think that before starting

eating the pudding, people have no clue what we are talking about. A lack

of frame of reference. People just don't hear what we are saying. Besides,

what we are saying is so simple that it cannot be true.

Still a big marketing problem. So many projects that can be saved and

hardly anybody understanding that we can do something about it.

Niels

✉ **Re: Yet another canceled public sector IT project ([R-24.49](#))**

<Jack Ganssle <jack@ganssle.com>>

Mon, 11 Dec 2006 08:05:19 -0500

Richard Karpinski complained that projects fail when we expect to be able to nail down all of the requirements up front, rather than embrace an

incremental approach as advocated by Tom Gilb and many others. Yet this reflects the essential tension in software development. He's right; realistically it's hard and sometimes impossible to understand the requirements early in the project. Yet he's wrong: management needs a price, up front, to decide if the project is at all affordable, and if the promised value exceeds development costs. Management needs a date, up front, to know if the product will hit the market window. We can waffle and promise to deliver a range of dates and costs, or we can protest mightily that such expectations are unreasonable. Yet if the project is late, so there's no revenue being generated, and as a result our paycheck is a dollar short or a day late, we go ballistic.

Alas, I fear this conundrum will never be resolved.

Jack Ganssle, jack@ganssle.com 410-504-6660 Skype jack.ganssle

🔥 **Re: Yet another canceled public sector IT project ([R-24.49](#))**

<Rex Black <rexblack@ix.netcom.com>>

Tue, 12 Dec 2006 08:05:42 +1300

I have a great deal of respect for Tom Gilb, who I consider a personal friend as well as an esteemed colleague. Also, I realize that these iterative lifecycle models are very popular right now.

That said, this heavy emphasis on these types of lifecycle models represent the latest manifestation of what Fred Brooks described as software engineering's "silver bullet" quest. A number of years ago, during the deflation of the 4GL bubble, which, ironically, overlapped the early days of object-oriented languages, Boris Beizer wrote mockingly in Latin about the "lingua salvator est" tendency, a desire to see the adoption of the right language as the magic solution, the savior, the discovery that would make all our problems go away. And, while we're on that note, CMM and TQM, anyone?

I am not saying that good languages, good processes, and a focus on quality are useless. I am saying that holding any *one* thing out as a solution is counter-productive at best.

Software engineering is hard for a number of reasons. Some of those reasons result from doing things we (collectively) know to be stupid. Others result from dogmatically following approaches laid out by others without regard for how to tailor those approaches to our situation. Let's not pretend that something as simple as a lifecycle model is going to solve all our problems, particularly when the real magic of a lifecycle model--if there is any magic in it--lies in tailoring it to what we really need.

Amer. Software Testing Qualifications Board, Int'l Software Testing Qual. Board, ... Bulverde, TX 78163 USA +1-830-438-4830 www.rexblackconsulting.com

Re: Yet another canceled public sector IT project (Black, [R-24.49](#))

<Richard Karpinski <dick@cfcl.com>>

Tue, 12 Dec 2006 16:20:24 -0800

> That said, this heavy emphasis on these types of lifecycle models

> represent the latest manifestation of what Fred Brooks described as

> software engineering's "silver bullet" quest.

Tom Gilb, in his 474 page "Competitive Engineering" is not offering a silver or magic bullet but rather a fleet of magic bulldozers, viewing lenses, decision processes, evaluation techniques, and an overarching focus on delivering measured value to identified stakeholders, including the users of the proposed system. The radically small steps allowed between instances of facing reality again, with usable deliveries to stakeholders, guarantees that if failure occurs, then it happens clearly in the first tenth of the project, not hidden until years of effort have been invested.

> A number of years ago, during the deflation of the 4GL bubble, which,

> ironically, overlapped the early days of object-oriented languages,

The early days of object-oriented languages was the mid 1960's for me with SIMULA-67.

> Boris Beizer wrote mockingly in Latin about the "lingua salvator est"

> tendency, ...

We have never before had a system like Planguage, where the magic was so thoroughly inspected, evaluated, guided, and verified in routine use of a "single" "language".

> And, while we're on that note, CMM and TQM, anyone?

You won't get me to disdain TQM since it seems to me that that is pretty close to SQC as advocated to such success in Japan by W. Edwards Deming whom I respect greatly.

> ... I am saying that holding any *one* thing out as a solution is counter-productive at best.

If you think Competitive Engineering is one thing, or that Tom's Planguage is just a good language for designing a project, then you need to read more of those 474 pages.

> Software engineering is hard for a number of reasons. ...

Which is exactly why the non-simple approach taken in Competitive Engineering is both demanding and successful. The very essence of the method is the focus on tailoring to the actual circumstances and measuring the success of applying engineering effort toward the identified measurable business goals of the project. In order to take advantage of all that tailoring and measuring, it is absolutely vital to avoid even medium sized development cycles.

Obviously, the best approaches will naturally avoid doing the things we know to be stupid. Since fixing the steps of the project at the very

beginning is
one of those really stupid ideas, I felt the need to rail
against it. But I
had to do it in a page or so to be published and read.

My view is that we actually will need many more pages than Tom
used to
explain his approach so that it can be understood without intense
consideration of each paragraph. But he had to do it in a form
that could
still be lifted without violating OSHA rules even when made
manifest on
printed paper.

Perhaps I'm unfairly picking on what you said. Clearly, I have
some skill in
treading on people's toes, despite a lack of conscious intent.
Would you
care to check in with Tom or Kai or Niels Malotaux to see what
they say
about your assertions?

Richard Karpinski, World Class Nitpicker
148 Sequoia Circle, Santa Rosa, CA 95401
dick@cfcl.com Home +1 707-546-6760 Cell +1 707-228-9716

⚡ Re: Slade on "Kim" ([RISKS-24.49](#))

<attilatthehun1900@tiscali.co.uk>
Mon, 11 Dec 2006 12:21:34 +0000

Rob Slade hits it right on the nose with his review of Rudyard
Kipling's
"Kim". Kipling was definitely one of us. In his "Just So
Stories", he
provided his "Six Honest Serving Men", the key question starters
that every
information security analyst and auditor worth their salt always

uses:

"I keep six honest serving-men
(They taught me all I knew);
Their names are What and Why and When
And How and Where and Who"

Michael "Streaky" Bacon

[Brent J. Nordquist notes that Project Gutenberg has the free
E-text. PGN]

<<http://www.gutenberg.org/etext/2226>>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 52

Thursday 21 December 2006

Contents

- [Report blames Denver election woes on flawed software](#)
[PGN](#)
- [Digital cameras converted to weapons](#)
[Mark Brader](#)
- [Secure Passports and IT Problems](#)
[Diomidis Spinellis](#)
- [RFIDs in Malaysian license plates](#)
[PGN](#)
- [An Ominous Milestone: 100 Million Data Leaks](#)
[ACM TechNews](#)
- [Risks of using spelunker's tools inside the genome](#)
[Denise Caruso](#)
- [Re: Yet another canceled public sector IT project](#)
[Steve Taylor](#) [Richard Karpinski](#)
- [Re: Flat train wheels](#)
[Olivier MJ Crepin-Leblond](#)
- [Re: Trig error checking](#)
[Mike Martin](#) [Richard A. O'Keefe](#) [Dik Winter](#) [PGN](#)

● [USENIX Annual Tech '07 Call for Papers](#)

[Lionel Garth Jones](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ Report blames Denver election woes on flawed software

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

Fri, 15 Dec 2006 10:30:17 PST

[Thanks to Gene Spafford for spotting this one.]

November 2006 Election Day problems in Denver were attributed to flawed ePollBook software from Sequoia Voting Systems ("decidedly subprofessional architecture and construction"). A consultants' report said "The ePollBook is a poorly designed and fundamentally flawed application that demonstrates little familiarity with basic tenets of Web development." Local election officials were also slammed for their "casual approach" to important technology. Source: Todd Weiss, *ComputerWorld*, 13 Dec 2006 <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9006038>

⚡ Digital cameras converted to weapons

<msb@vex.net (Mark Brader)>

Tue, 12 Dec 2006 17:29:25 -0500 (EST)

One of the quotes in my signature collection reads: "Every new technology

carries with it an opportunity to invent a new crime." That was Laurence Urgenson (an assistant chief US attorney), speaking in 1987 about the first arrests for what was later called cellphone cloning.

Well, here's another example of criminal technological improvisation: electric shock weapons, like a Taser, produced by teenagers from disposable digital cameras!

<http://www.cbc.ca/canada/edmonton/story/2006/12/12/teens-cameras.html>

Mark Brader, Toronto, msb@vex.net

✶ Secure Passports and IT Problems

<Diomidis Spinellis <dds@aueb.gr>>
Wed, 13 Dec 2006 13:12:38 +0200

In 2003 Greece, in response to new international requirements for secure travel documents, revised the application process and contents of its passports. From January 1st 2006 passports are no longer issued by the prefectures, but by the police, and from August 26th passports include an RFID chip. The new process has been fraught with problems; many of these difficulties stem from the IT system used for issuing the passports. On December 12th, the Greek Ombudsman (human rights section) issued a special 22-page report on the problems of the new passport issuing process. The

report is based on 43 official citizen complaints.

In the report's introduction the Ombudsman stresses the sinister symbolism of transferring the authority for issuing passports to the police - a body organized under quasi-military principles: international travel has nowadays become mainly a security issue. The Ombudsman details many procedural problems of the new process. At least three of them appear to be related to the new IT system handling the passport application.

1. The system used can't handle the correct entry of some names, apparently because it doesn't support some characters or symbols, like the hyphen.

2. If a passport application is rejected, and the citizen subsequently appeals successfully against that decision, the IT system doesn't offer a way to resubmit the original application; a new application has to be completed and submitted.

3. The passport IT system appears to have been linked against databases containing the details of wanted persons, such as fugitives and those with pending penalties. Thus persons appearing in the wanted person database get arrested when they go to a police station to apply for a passport. According to the Ombudsman, this is problematic for two reasons. First, the data in the wanted person file may be wrong. Second, through this procedure the police performs a blanket screening of all citizens that wish to exercise their right to travel outside the country. Paradoxically, one

other database, that listing persons actually prohibited to leave the country, is not consulted when the application is filed.

In sum the Ombudsman finds that the new system of issuing passports emphasizes the security of the travel documents at the expense of citizens' rights, decent governance, and efficiency.

The report also contains recommendations for minimizing the effects of the current seasonal rush, which has resulted in queues forming at 3:30 in the morning. The Ombudsman recommends a system for setting up appointments by phone and the addition of seasonal staff. However, an obvious way of streamlining the process is overlooked. Currently citizens fill-in data entry application forms. Police officers then enter the details from the forms into the IT system; typically at a snail's pace, because most of them can't touch-type. The whole process can easily last 15-20 minutes for a single application. Allowing the citizens to complete the forms on-line, would allow the police officers to print the forms from a reference number supplied by the applicant, and have them signed in person. This would speed up many of the applications and would also eliminate transcription errors.

Diomidis Spinellis - Athens University of Economics and Business
<http://www.dmst.aueb.gr/dds>

RFIDs in Malaysian license plates

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

Sat, 9 Dec 2006 12:55:02 -0500

[Thanks to Marc Rotenberg for this one.]

Malaysia to embed car license plates with microchips to combat theft

The Associated Press, 8 Dec 2006

http://www.iht.com/articles/ap/2006/12/09/asia/AS_GEN_Malaysia_Car_Thefts.php

Malaysia's government, hoping to thwart car thieves, will embed license plates with microchips containing information about the vehicle and its owner, a news report said Saturday. With the chips in use, officials can scan cars at roadblocks and identify stolen vehicles, the *New Straits Times* reported. The "e-plate" chip system is the latest strategy to prevent car thieves from getting away with their crimes by merely changing the plates, the report said. (Nearly 30 cars -- mostly luxury vehicles -- are stolen every day in Malaysia.) ... The microchips, using radio frequency identification technology, will be fixed into the number plates and can transmit data at a range of up to 100 meters (yards), and will have a battery life of 10 years.

⚡ An Ominous Milestone: 100 Million Data Leaks

<TechNews <technews@ACM.ORG>>

Mon, 18 Dec 2006 14:05:25 -0500

Wired News senior editor Kevin Poulsen announced on his blog last Thursday that with announcements from UCLA (800,000 records stolen), Aetna (130,000 records stolen) and Boeing (320,000 records stolen), over 100 million records had been stolen since the ChoicePoint breach almost two years ago. While perpetrators of the Aetna and Boeing laptop thefts were probably not after personal records, the same cannot be said for the UCLA data theft, where a hacker had been accessing the university's database of personal information for over a year before being discovered. A Public Policy Institute study, using data from the Identity Theft Resource Center, showed that of the 90 million records stolen between 1 Jan 2005, and 26 Mar 2006, 43 percent were at educational institutions. ...

✶ Risks of using spelunker's tools inside the genome

<Denise Caruso <caruso@hybridvigor.org>>

Wed, 20 Dec 2006 10:47:40 -0800

I just published a book called 'Intervention: Confronting the Real Risks of Genetic Engineering and Life on a Biotech Planet.' (Details at <http://hybridvigor.org/intervention>.) It focuses on the flaws in risk assessment methods for innovations in science and technology, specifically the scientific uncertainties that biotech risk evaluations dismiss or ignore.

While a lot of the issues are pretty much straight-up biology and public-policy atrocities, there are several technical foibles in the brave new world of industrial genomics that are in serious need of some attention. I ended up cutting most of them out of the book because of excessive nerditude from the layperson's perspective, but I thought RISKS folk might find them interesting.

1. 95 percent of the gene-disease links that make headlines every time

they're reported (i.e., the gene for diabetes, Alzheimer's, obesity,

schizophrenia, depression, and many others) are false positives,

attributed to the speed and efficiency with which new equipment can

automatically sequence and analyze genes. Since "reading" genes can take

about a day now instead of several months, thousands of them at a time can

be scanned quickly. But because the sequences are analyzed in bulk and

quickly, some of them by chance alone seem linked to a disease in a

statistically significant way even though they aren't.

2. There are no standards for PCR equipment, the machines that can

synthetically "amplify" or reproduce a single DNA sequence into a few

bazillion identical sequences. It's so key to research that it's been

called the "duct tape" of genomics. Virtually every genetics experiment

uses PCR. But PCR is ultrahypersensitive, a situation that's exacerbated

by way the equipment itself performs. It's not just that results of DNA

measurements from experiments performed on different PCR platforms are not

necessarily comparable. One NIST staffer says that results may not be

repeatable *even with the same equipment.*

3. For another lab workhorse, the "gene chip," the problem seems simply to

be that it isn't sensitive enough. Gene chips are based on a different,

far less sensitive technology than PCR called hybridization.

Hybridization is like having 20-20 tunnel vision -- it does great within

its limited range, but it can detect absolutely nothing outside it. What

gene chips can produce is a false negative result. False negatives in

other kinds of tests would indicate that test subjects don't have HIV,

when they do. Or that anthrax DNA isn't present on the envelope in the

Senate mailroom, when in fact it is. In the context of risk and in the

most obvious example -- genetic contamination -- the ability to detect a

specific DNA or RNA sequence, or to be able to notice that a certain gene

is not being expressed, would be a key element in determining whether or

not there's cause for alarm.

With so many different points in the scientific process where the tools

themselves can introduce fundamental errors in the data, it doesn't seem out

of the question to ask what research results might be overlooking, mistaking

for something else, or simply not seeing at all.

I'd like to see this whole area broken wide open. In my opinion, we are

messing around with the fundamental building blocks of living organisms

using tools that look very sophisticated, but seem to me more like the

equivalent of a spelunker's lamp and a pick and shovel.

Denise Caruso, Executive Director, The Hybrid Vigor Institute
<http://hybridvigor.org> Blog: <http://hybridvigor.net>

[We have long been concerned here with the risks of overendowing risk assessment techniques -- and especially quantitative approaches -- along with the risks of misusing the results of such analyses.

Although

Denise's book might seem to be less computer related than many other

topics discussed in RISKS, I think there are many problems and lessons to

be learned from what we have in common. It is important for everyone to

see that these problems are generic and relevant to essentially all

technologies, not just computer systems. PGN]

✉ **Re: Yet another canceled public sector IT project ([R-24.49](#))**

<"Steve Taylor" <steve.taylor@assetcods.com>>

Mon, 18 Dec 2006 15:45:21 -0000

The commentary on this item so far has been quite interesting and I believe does address a key reason for why so many public projects fail. Unfortunately, here in the UK at least and I suspect elsewhere as well, there are serious problems with public projects using incremental development. The UK OGC (Office of Government Commerce) has been promoting "stronger" contracts between government and suppliers. These have now become quite onerous and they create a situation where the whole project is

managed in a legalistic way. This results in both sides focusing very strongly on the original requirements as specified at time of contract. The incorporation of changes is seen by both sides as an opportunity for the supplier to make some real money and as such is subject to a rigorous and expensive change management procedure. The overall effect is to act as a brake on any change preventing all but the most important changes taking place. The end result is all too easy to predict and the trend is in completely the opposite direction to those being suggested.

The only way out of this mess is for government and their suppliers to find a more cooperative model for operating these projects. I strongly believe incremental development is the way to go and it would be sensible for suppliers to use it but in all too many cases there is insufficient flexibility in the requirements. The suppliers best interests are served by doing what they agreed to do rather than something that will work. Even where a supplier is willing to be helpful the purchasing body will often make the administrative cost of supplier suggested changes so high that none are suggested.

✉ Re: Yet another canceled public sector IT project (Ganssle, [R-24.49](#))

<Richard Karpinski <dick@cfcl.com>>
Sat, 16 Dec 2006 15:42:13 -0800

Management needs to learn more about projects so they don't fall into that trap. They can't get and don't need a price, and if they believe in one that they are given, then they should immediately resign as they have already demonstrated their incompetence. All they need to know is that the initial budget is affordable and that the initial steps of the project will probably deliver results whose value is likely to exceed the costs.

There is certainly some attraction to the notion that the whole project can be understood and guaranteed before any budget is allocated, but it is completely obvious that such notions are unrealistic and misleading. Management needs to manage, not only at the start of the project, but at many other times before the project completion date is reached.

> Management needs a date, up front, to know if the product will hit the
> market window. We can waffle and promise to deliver a range of dates and
> costs, or we can protest mightily that such expectations are unreasonable.

I protest mightily. Even if they get a date, they cannot realistically believe it. Even if they could believe it, they cannot be assured that the market window will appear at the scheduled time. Fixing the product definition, cost, and timing all in advance of the beginning of the project is manifest foolishness.

Give engineering a chance to work, a chance to trade off one detail against

another to maximize the value delivered to stakeholders. This does make the resulting product less clear at the start of the project, but it IS less clear than the advocates would have you believe. This is to say, the reality is more unknowable than the advocates aver.

Skepticism is a required feature of good management practices. When a proposal claims that a two or three year project can be accurately and adequately defined and implemented with a knowable budget and that the result will have a knowable value when it is delivered, years in the future, the only proper management response is to laugh that proposal out of the room.

> Yet if the project is late, so there's no revenue being generated, and as
> a result our paycheck is a dollar short or a day late, we go ballistic.

If that were the only reason for no revenue being generated, this world would be very much easier to understand and deal with. In fact the major reason that no revenue is generated is that the project designers did not plan for any revenue to be generated until the project is completed and all the money spent.

Many projects are not intended to produce a product to be marketed and then ignored. In these cases, usable deliveries of improvements can generate revenue, or value, long, long before the completion of the entire project. Neglecting this fact is failing to accomplish the due diligence aspect of management.

I suspect that many customers who recognize the need for a product to accomplish X will be only too happy to PAY for a product which does only a portion of the whole task, if it will be improved monthly or quarterly as guided by customer feedback. This notion needs some testing and validation, but several recent works stress the value of carrying on a two way conversation with your customers. See "The Clue Train Manifesto" for example.

> Alas, I fear this conundrum will never be resolved.

Probably true, but that does not mean it cannot be addressed and managed to accomplish substantial improvements in project management and substantial reduction of the risks involved. Such gains require non-traditional approaches but they do not require silver bullets or magic or slavish adherence to some particular method. They only require open minds, brave hearts, skepticism, and common sense. Would we had more of those.

Richard Karpinski, 148 Sequoia Circle, Santa Rosa, CA 95401
dick@cfcl.com

+1 707-546-6760 "nitpicker" in subject line gets past my spam filters.

Re: Flat train wheels (Ladkin, [RISKS-24.51](#))

<"Olivier MJ Crepin-Leblond" <ocl@gih.com>>
Sun, 17 Dec 2006 00:27:41 +0100

> In Fall, in areas with deciduous trees, a slippery film
deriving
> from mulched fallen leaves can build up on rails.

More than this, it is a mulch that develops on the wheels
themselves that
make them slip. The problem appeared in the UK on most new
trains which had
"new" (at the time) breaking systems consisting of disc brakes,
or pads
rubbing the *side* of the wheel. British Rail engineers found
that the
problem was less likely on older trains where the brake pads
would be
applied to the rolling surface of the wheel itself (the
circumference), thus
scrubbing the rolling surface clean of all the mulch every time
the brakes
were applied.

Definitely a case where new technology is introducing new
problems.

Olivier MJ Crepin-Leblond, Ph.D. <ocl@gih.com> Tel:+44 (0)7956
84 1113

[This leaves mulch to be desired. PGN]

✉ Re: Trig error checking (Ewing, [RISKS-24.51](#))

<"mike martin" <mke.martn@gmail.com>>
Mon, 18 Dec 2006 21:27:26 +1100

Martin Ewing wrote of a VAX floating point unit that exhibited
intermittent
faults ([RISKS-24.51](#) <<http://catless.ncl.ac.uk/Risks/24.51.html>>). Computers'

arithmetic-logic units ((ALUs) don't seem well protected against intermittent faults. In the early 1970s I worked with a Burroughs B6700 computer that occasionally, when compiling a copy of its operating system, failed the computation with a spurious fault. (The core operating system was written in an Algol dialect and took about 20 minutes to compile.)

After much investigation we found that the cause was an occasional bit dropped by the RDIV operator (which calculated the remainder from an integer division). This rarely used operator was used by the operating system in calculating disk segment addresses in the computer's virtual memory paging file. When a bit was dropped in the segment address, the compiler would be fed a chunk of garbage from the wrong page file segment and flag a syntax error. After some detective work I wrote a program that did repeated RDIVs and checked the results, highlighting the problem. The fault was rare, less than once in 1000.

Had the problem occurred with a more commonly used operator the result could have been nasty.

Perhaps ironically this was one of the first B6700s that was delivered with main memory that included Hamming code single bit error correction and double bit error detection. But nothing detected a faulty ALU.

Mike Martin mke.martn@gmail.com
Sydney

⚡ Re: Trig error checking (Ewing, [RISKS-24.51](#))

<"Richard A. O'Keefe" <ok@cs.otago.ac.nz>>
Tue, 19 Dec 2006 14:01:56 +1300 (NZDT)

I used to work at Quintus, who then made a Prolog compiler. We were keen to get our product in the catalogues of various computer vendors. One such vendor had a policy of thoroughly testing programs before accepting them into their catalogue. So one fine day a bug report from them landed on my desk: such-and-such a trig function was delivering answers that were slightly off. That's odd, I thought: I wrote that code and it just calls their code through the foreign interface, I wonder what happens if I call that from C? You guessed it: the bug was in their code. They were testing other people's code much more thoroughly than their own.

⚡ Re: Trig error checking (Ewing, [RISKS-24.51](#))

<Dik.Winter@cw.nl>
Sun, 17 Dec 2006 03:33:54 +0100 (MET)

Mark Ewing:

> Eventually we found that our
> VAX floating point unit (a very large circuit board) was malfunctioning. It
> gave slightly wrong results, but quietly - there were no system error

> reports. The diagnostic was that $\sin^2 + \cos^2$ was
intermittently not
> quite equal to 1 for various arguments. [NOTE: This is a
positive example
> of circular reasoning! PGN]

Indeed. Even with an optimal implementation of \sin and \cos it
is not
necessarily the case that $\sin^2 + \cos^2$ equals 1. It is
likely, but
not necessary. Consider an angle of 45 degrees. In IEEE single
precision the best approximation to $\sqrt{2}/2$ is (in binary):
0.1011010100000100111110010
the square of that is (with proper rounding):
0.10000000000000000000000001
not really equal to $1/2$, and I think that similar examples can
be created
using radian arguments. This one also does not work in IEEE
double
precision. (And if you want to check with a program, be sure
that after
each individual operation the result is rounded to the precision
you
operate with and that you do use that rounded result. Otherwise
you
will see discussions I have had already a long time ago about
another
problem with floating-point arithmetic.)

There is a lot of relevance here. Assuming that mathematical
relations
also hold when doing floating-point arithmetic on computers can
lead to
errors. There is a whole field of mathematics devoted to just
this
(numerical mathematics).

> Field service got us new boards, but how could we have
confidence this bug
> was not recurring? In the end we ran a background routine
that checked
> $\sin^2 + \cos^2$ forever. (Today, we would make it a
screensaver program.)

I do not think you checked for the whole range, otherwise you would have found errors forever.

> There is a RISKS issue -- how do you know your CPU is giving good results?

> There aren't any check bits for trig functions.

Trust. Already quite some time ago (1970?) Cody and Waite wrote a book

that contained programs that would check the basic elementary functions.

There also does exist an elementary program that checks the basic arithmetic of computers (from memory, "elefun" by Kahan). But even these

did not help with the Pentium bug. And, of course, some basic knowledge about numerical mathematics.

dik t. winter, cwi, kruislaan 413, 1098 sj amsterdam, nederland, +31205924131

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

⚡ Re: Trig error checking (Ewing, [RISKS-24.52](#))

<RISKS List Owner <risiko@csl.sri.com>>

Thu, 21 Dec 2006 12:01:27 PST

Of course, an incorrect $\cos(x)$ could have been computed from an incorrect $\sin(x)$ as

$$\sqrt{1 - [\sin(x)]^2}$$

in which case the sum of the squares would be IDENTICALLY 1,

modulo
roundoff errors. So that check is NOT ENOUGH.

[Incidentally, I put a correction to Martin's note in [RISKS-24.51](#),
changing "1990s" to "1980s" on the date of the VAX episode.
PGN]

USENIX Annual Tech '07 Call for Papers

<Lionel Garth Jones <lgj@usenix.org>>
Thu, 21 Dec 2006 10:58:20 -0800

Call for Papers
2007 USENIX Annual Technical Conference
June 17-22, 2006, Santa Clara, CA
Paper Submissions Deadline: January 9, 2007
<http://www.usenix.org/usenix07/cfpa/>

On behalf of the 2007 USENIX Annual Technical Conference program committee,
we request your ideas, proposals, and papers for tutorials,
refereed papers,
and a poster session.

The program committee invites you to submit original and innovative papers to the Refereed Papers Track of the 2007 USENIX Annual Technical Conference. Authors are required to submit full papers by 11:59 p.m. PST, Tuesday, January 9, 2007.

We seek high-quality submissions that further the knowledge and understanding of modern computing systems, with an emphasis on practical implementations and experimental results. We encourage papers that break new ground or present insightful results based on experience with

computer systems. The USENIX conference has a broad scope.

Specific topics of interest include but are not limited to:

- * Architectural interaction
- * Benchmarking
- * Deployment experience
- * Distributed and parallel systems
- * Embedded systems
- * Energy/power management
- * File and storage systems
- * Networking and network services
- * Operating systems
- * Reliability, availability, and scalability
- * Security, privacy, and trust
- * System and network management
- * Usage studies and workload characterization
- * Virtualization
- * Web technology
- * Wireless and mobile systems

More information on these and other submission guidelines is available on our Web site:

<http://www.usenix.org/usenix07/cfpa/>

IMPORTANT DATES:

Paper submissions due: Tuesday, January 9, 2007, 11:59 p.m. PST

Notification to authors: Monday, March 19, 2007

Final papers due: Tuesday, April 24, 2007

Please note that January 9 is a hard deadline; no extensions will be given.

We look forward to your submissions.

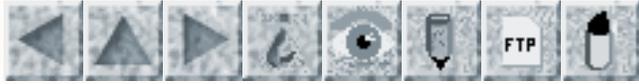
On behalf of the Annual Tech '07 Conference Organizers,

Jeff Chase, Duke University

Srinivasan Seshan, Carnegie Mellon University

2007 USENIX Annual Technical Conference Program Co-Chairs

usenix07chairs@usenix.org



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 53

Friday 29 December 2006

Contents

- [Glitches postpone launch at Wallops](#)
[Walter Schilling](#)
- [Cybercrooks Deliver Trouble ...](#)
[Brian Krebs via Monty Solomon](#)
- [Typo takes tourist 13,000 km out](#)
[Monty Solomon](#)
- [2007 Preview: Newt's Muzzle, Google's Data, Microsoft Over the Line](#)
[Lauren Weinstein](#)
- [Vista DRM The 'Longest Suicide Note in History'?](#)
[Peter Gutmann via Gunnar Helliesen and Dave Farber](#)
- [Drop zones and an intelligence war](#)
[Gadi Evron](#)
- [Re: Trig error checking](#)
[Ted Lee Ken Knowlton Gene Spafford](#)
- [Re: Flat train wheels](#)
[Peter B. Ladkin](#)
- [E-mail me at xx at yy dot zz](#)
[Dan Jacobson](#)

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

Glitches postpone launch at Wallops Island

<Walter Schilling <walter.schilling@computer.org>>

Fri, 22 Dec 2006 21:24:37 -0500

It appears that software coupled with a fast cycle development time for spacecraft has again resulted in a launch problem. While the details of this article are sketchy at best, it harkens back to the Milstar 3, ICO Global Communications F-1 Satellite, GeoSat, and Clementine failures.

<http://www.baltimoresun.com/news/nationworld/bal-te.wallops12dec12,0,5583500.story>

Walter W. Schilling, Jr., 2004-2007 Ohio Space Grant Consortium, Doctoral Candidate, University of Toledo, Department of EECS

Cybercrooks Deliver Trouble ...

<Monty Solomon <monty@roscom.com>>

Wed, 27 Dec 2006 20:53:15 -0500

With Spam Filters Working Overtime, Security Experts See No Letup in '07,
Brian Krebs, *The Washington Post*, 27 Dec 2006

It was the year of computing dangerously, and next year could be worse.

That is the assessment of computer security experts, who said

2006 was marked by an unprecedented spike in junk e-mail and more sophisticated Internet attacks by cybercrooks.

Few believe 2007 will be any brighter for consumers, who already are struggling to avoid the clever scams they encounter while banking, shopping or just surfing online. Experts say online criminals are growing smarter about hiding personal data they have stolen on the Internet and are using new methods for attacking computers that are harder to detect. "Criminals have gone from trying to hit as many machines as possible to focusing on techniques that allow them to remain undetected on infected machines longer," said Vincent Weafer, director of security response at Symantec ...

One of the best measures of the rise in cybercrime is junk e-mail, or spam, because much of it is relayed by computers controlled by Internet criminals, experts said. More than 90 percent of all e-mail sent online in October was unsolicited junk mail, according to Postini, an e-mail security firm in San Carlos, Calif. Spam volumes monitored by Postini rose 73 percent in the past two months as spammers began embedding their messages in images to evade junk e-mail filters that search for particular words and phrases. In November, Postini's spam filters, used by many large companies, blocked 22 billion junk-mail messages, up from about 12 billion in September.

The result is putting pressure on network administrators and corporate

technology departments, because junk mail laden with images typically requires three times as much storage space and Internet bandwidth as a text message, said Daniel Druker, Postini's vice president for marketing. ...

<http://www.washingtonpost.com/wp-dyn/content/article/2006/12/26/AR2006122600922.html>

✶ Typo takes tourist 13,000 km out

<Monty Solomon <monty@roscom.com>>

Fri, 29 Dec 2006 12:42:40 -0500

Typo takes tourist 13,000 km out, Reuters, 29 Dec 2006

A 21-year-old German tourist who wanted to visit his girlfriend in the Australian metropolis Sydney landed 13,000 kilometers (8,077 miles) away near Sidney, Montana, after mistyping his destination on a flight booking Web site. ...

<http://www.cnn.com/2006/WORLD/europe/12/29/germany.tourist.reut>

✶ 2007 Preview: Newt's Muzzle, Google's Data, Microsoft Over the Line

<Lauren Weinstein <lauren@vortex.com>>

Thu, 21 Dec 2006 15:24:40 -0800

2007 Preview: Newt's Muzzle, Google's Data, and Microsoft Over the Line

(<http://lauren.vortex.com/archive/000204.html>)

Greetings. As 2006 draws to a close, I wanted to review three issues from this year that are likely to be of considerable note in 2007. One is a bizarre blast from left field (or more precisely "right field"), the next is a pressure cooker data problem that we must resolve soon, and the last demonstrates how anti-piracy efforts can cross the line from reasonable to arrogant and potentially dangerous.

The latter two of these topics may cry out for legislative attention if voluntary approaches continue to be impotent -- and with the new Congress coming into power we may have our best shot of accomplishing something positive on the federal level if legislation indeed becomes necessary.

I realize that many people shudder at the prospect of legislation, fearing that it may make matters worse, that lobbyists will warp beneficial efforts into twisted mutations of intent, and similar concerns. These are indeed real risks, but we're also seeing the increasing risks of allowing important technology issues that affect society at large to be determined solely by corporate entities who -- quite naturally and understandably -- have their own agendas and priorities. Again, I'd prefer to see things done on a voluntary basis, but we may have to bite the bullet and give legislation the old college try.

But onward to the issues ...

OK, what the blazes is Newt's Muzzle? A couple of weeks ago, former Speaker of the House Newt Gingrich started spouting off (first in a speech and just a few days ago on NBC's "Meet the Press") about how useful it would be to censor the Internet. The example he's using (for now) is "jihadist" Web sites, and he'd like a panel of federal judges to decide which sites would be "closed down."

Outside of showing his true colors when it comes to freedom of speech issues, Newt is also displaying a woeful lack of understanding of the Internet and how essentially impossible (and counterproductive) attempts at censorship really are in this environment.

The UK Guardian asked me for an op-ed on this topic, and it went up on their Web site a few days ago as "Can Newt Nix the Net" (<http://www.pfir.org/guard-newt-oped>). Rather than my taking much more space discussing the matter here, if you're interested in Newt's thinking (and my views on the Internet censorship topic in this context), please visit that link.

Even though Internet censorship (despite the help of U.S. technology companies that provide systems to foster its deployment) is ineffective, it is still a tremendously counterproductive waste of time, resources, and human creativity, and distorts communications in ways that are both unnecessary and potentially result in dangerous backlashes. This is an issue that will only become more important in 2007 and beyond.

Onward ...

The data retention controversy -- the battle to determine how much data is reasonable for search engines and other entities to maintain on their users -- is becoming ever more a red flag issue. In 2006 alone we saw the specter of the feds going after Google data in DOJ vs. Google, AOL releasing privacy-invasive search keyword lists, and issues of Chinese use of U.S. company Internet records to track dissidents, among other similarly distressing activities.

The concerns in this area go way beyond Google, but as the most powerful player in the Internet search industry, Google has a special responsibility to be a leader, not only by fulfilling their "don't be evil" slogan (and I do believe Google's motives are benign) but also by not creating infrastructures that allow others to do evil. It is in this latter respect that it appears Google "talks the talk" when it comes to concern about how their data could be abused by outsiders, but hasn't "walked the walk" by taking sufficient definitive steps to make such abuse impossible.

Again, I'd prefer that this entire area (industry-wide, not just Google) be dealt with on a voluntary basis. But as I've discussed in detail over at the California Initiative For Internet Privacy (<http://www.cifip.org>) and links referenced there, if voluntary approaches don't work we may have to take the next step, either at the California initiative level or -- given the upcoming changes in Congress -- perhaps at the federal legislative level

(an option that did not appear reasonably to be on the horizon when I wrote the existing CIFIP essay). While some of my reservations about the California state legislature might apply to Congress as well, it is undeniable that a federal approach to these issues could be far more effective, that is if -- and only if -- we need to choose the legislative course.

This is a complex area, with the competing goals of mandated data destruction to protect users' privacy, and the desires of governments to mandate data retention, continuously at odds. We have a tremendous amount of work to do to reach a reasonable outcome.

Finally ...

There's been a lot of discussion about the anti-piracy features in Microsoft's new "Vista" Windows operating system (e.g. <http://lauren.vortex.com/archive/000194.html>). I've had a number of very friendly conversations with MS executives regarding the issues surrounding their anti-piracy implementations, and in particular their new ability to functionally "hobble" Vista systems that they believe are pirated.

The more that I've considered this, the increasingly unreasonable and hazardous this functionality appears to be. It turns the assumption of innocence on its head -- you have to take affirmative steps to prove to Microsoft that you're not a pirate if your system appears on their suspect hit list. As we know from Windows XP, there are all sorts of

ways that honest consumers can end up with systems that have cloned copies of the OS (often installed by repair depots to replace trashed copies of the original system after disk failures, for example).

Many consumers don't even realize the difference between the hardware and operating system of their computers. Many will ignore the warning messages that MS will send before triggering a system hobble, assuming that the messages don't apply in their cases, or that they're phishing or virus come-ons. The mere existence of the mechanisms to initiate the hobbling may represent an attractive attack vector for destructive hackers, who might well get their jollies by shutting down a few thousand (million?) PCs at a time.

Vast numbers of these computers will be in highly important applications in business, health care, government, and the military. Yes, Microsoft says you're not supposed to use them for critical applications. But we know what the real world looks like, and even the definition of "critical" can be nebulous.

Even more to the point (and this also relates to the data retention issues above) it is extremely problematic to assume that it is even reasonable for individual corporate entities to have total ad hoc, carte blanche authority to make these decisions on their own, decisions that technologically have an enormous and ever increasing impact on individuals and society at large.

I might add that while the new Microsoft anti-piracy systems are of particularly concern, there are other anti-piracy technologies being deployed that carry similar risks, including but not limited to a range of upcoming Digital Rights Management (DRM) systems.

I keep saying "voluntary is best" and I mean it. In all of these areas I've discussed, voluntary approaches are always to be preferred. But in our society, a key role of legislation is to help provide mechanisms for "power-sharing" in situations like these, if voluntary and cooperative approaches prove to be failures.

We are all part of this. We can sit on our hands and watch as spectators -- or we can get our hands dirty by reaching directly into the innards of the machines -- figuratively speaking -- and helping making sure that these systems serve not only their immediate masters, but also society's requirements as well.

None of this will be trivial, of course. But to quote the great animated philosopher "Super Chicken" -- "You knew the job was dangerous when you took it."

Have a great holiday season, and all the best for 2007. Take care, all.

Lauren Weinstein +1(818)225-2800 <http://www.pfir.org/lauren>
Blog: <http://lauren.vortex.com> DayThink: <http://daythink.vortex.com>

✦ Vista DRM The 'Longest Suicide Note in History'? (via Dave Farber IP)

<Gunnar Helliesen <gunnar@helliesen.com>>

December 26, 2006 3:50:46 PM EST

Highly recommended piece by security researcher Peter Gutmann. It details how Vista is intentionally crippled, to protect "premium content". Also possible effects on OSS, drivers and such. For IP, if you wish.

A Cost Analysis of Windows Vista Content Protection
Peter Gutmann, pgut001@cs.auckland.ac.nz

http://www.cs.auckland.ac.nz/~pgut001/pubs/vista_cost.txt

Last updated 27 December 2006

Executive Summary

Windows Vista includes an extensive reworking of core OS elements in order to provide content protection for so-called "premium content", typically HD data from Blu-Ray and HD-DVD sources. Providing this protection incurs considerable costs in terms of system performance, system stability, technical support overhead, and hardware and software cost. These issues affect not only users of Vista but the entire PC industry, since the effects of the protection measures extend to cover all hardware and software that will ever come into contact with Vista, even if it's not used directly with Vista (for example hardware in a Macintosh computer or on a Linux server). This document analyses the cost involved in Vista's content

protection, and the collateral damage that this incurs throughout the computer industry.

Executive Executive Summary

The Vista Content Protection specification could very well constitute the longest suicide note in history. [...]

Disabling of Functionality

Vista's content protection mechanism only allows protected content to be sent over interfaces that also have content-protection facilities built in. Currently the most common high-end audio output interface is S/PDIF (Sony/Philips Digital Interface Format). Most newer audio cards, for example, feature Toslink digital optical output for high-quality sound reproduction, and even the latest crop of motherboards with integrated audio provide at least coax (and often optical) digital output. Since S/PDIF doesn't provide any content protection, Vista requires that it be disabled when playing protected content. In other words if you've invested a pile of money into a high-end audio setup fed from a digital output, you won't be able to use it with protected content. Similarly, component (YPbPr) video will be disabled by Vista's content protection, so the same applies to a high-end video setup fed from component video. [...]

[Note: *The New York Times* had a Christmas-Day article on Vista flaws:

<http://www.nytimes.com/2006/12/25/technology/25vista.html?hp&ex=1167022800&en=67d067ceedf719aa&ei=5094&partner=homepage>

PGN]

🔥 Drop zones and an intelligence war (fwd)

<Gadi Evron <ge@linuxbox.org>>

Sat, 23 Dec 2006 12:32:49 -0600 (CST)

In this post (<http://www.phenoelit.net/lablog/Irresponsible.sl>),
FX
describes a drop zone for a phishing/banking trojan horse, and
how he
got to it.

Go FX. I will refrain from commenting on the report he describes
from Secure
Science, which I guess is a comment on its own.

We had the same thing happen twice before in 2006 (that is worth
mentioning
or can be, in public).

Once with a very large "security intelligence" company giving
drop zone data
in a marketing attempt to get more bank clients ("hey buddy, why
are 400
banks surfing to our drop zone?!?!)

Twice with a guy at DEFCON showing a live drop zone, and the
data analysis
for it, asking for it to be taken down (it wasn't until a week
later during
the same lecture at the first ISOI workshop hosted by Cisco).
For this guy's
defense though, he was sharing information. In a time where
nearly no one
was aware of drop zones even though they have been happening for
years, he
shared data which was valuable commercially, openly, and allowed
others to

clue up on the threats.

Did anyone ever consider this is an intelligence source, and take down not being exactly the smartest move?

It's enough that the good guys all fight over the same information, and even the most experienced security professionals make mistakes that cost in millions of USD daily, but publishing drop zone IPs publicly? That can only result in a lost intelligence source and the next one being, say, not so available.

I believe in public information and the harm of over-secrecy, I am however a very strong believer that some things are secrets for a reason. What can we expect though, when the security industry is 3 years behind and we in the industry are all a bunch of self-taught amateurs having fun with our latest discoveries.

At least we have responsible folks like FX around to take care of things when others screw up.

I got tired of being the bad guy calling "the king is naked"[*], at least in this case we can blame FX. :)

[* Especially when "the Emperor has no clothes." PGN]

It's an intelligence war, people, and it is high time we got our act together.

I will raise this subject at the next ISOI workshop hosted by Microsoft (<http://isotf.org/isoi2.html>) and see what bright ideas we come up with.

✉ Re: Trig error checking ([RISKS-24.51/52](#))

<"Ted Lee" <Ted.Lee@baesystems.com>>

Fri, 22 Dec 2006 10:13:36 -0600

Speaking of spurious faults, which "mike martin" <mke.martn@gmail.com> did in [RISKS-24.52](#), I am reminded of an amusingly insidious fault I ended up tracking down at the PDP-1 at the Cambridge Electron Accelerator ca. 1968. The machine was used primarily to run experiments, but one of the professors had the idea of also using it as a teaching aid. The machine had been retrofitted with memory protection hardware so several experimenters could run their software at once without stepping on each other's toes. (As I recall, it didn't have any address translation, just protection) I ran a program (n-body simulator for elementary physics classes) I'd written that had been working fine -- and it came up with a memory fault, repeatedly. I tracked the fault down to happening in a display subroutine, in particular, a subroutine to draw a circle. I vaguely remember simplifying everything so all I was doing was drawing a single large circle (like a foot in diameter -- the screen was huge) -- and the machine and display were slow enough I could see that the fault happened exactly at something like the top of the screen. The only "interesting" thing about that is that it was at a point

where the value in the accumulator would have been all 1's and on the next iteration overflowed to all 0's. For any of you old enough to know what a real computer was like, the buses in this machine were bundles of wires or flat cables with something like 18 wires in them. It turns out that the single wire (and it really was a single wire that just sort of hung across the electronic racks) that carried the signal indicating a protection violation had been routed close to the accumulator: the sudden energy of all the bits turning from 1 to 0 got coupled into that wire and caused the fault.

⚡ Re: Trig error checking ([RISKS-24.51/52](#))

<Ken Knowlton <KCKnowlton@aol.com>>

Fri, 22 Dec 2006 20:41:30 EST

The recall of lurking, obscure errors from olden times (ca 1960) brings to mind one struggle I had during the development of a system on the IBM 7090 (7094?) at MIT -- when my main debugging tool was a massive core dump of spaghettified list structure. After a week of bashing my head, I had a hunch: I asked the machine operators, between runs, manually to store a particular number in a certain register, fetch it, and see whether the nth bit got dropped. Three hours later I stopped by for the news: two out of five tries the 1 turned to 0.

Yes, stuff like that was happening with hardware as well as software; during my week of puzzlement (and earlier), who knows what how much trash was strewn into others' results?

✉ **Re: Trig error checking ([RISKS-24.51/52](#))**

<Gene Spafford <spaf@cerias.purdue.edu>>

Fri, 22 Dec 2006 14:35:05 -0500

Nearly 25 years ago, some of my grad school buddies were working on a compiler and support language as part of the Georgia Tech Software Tools project. This was a full set of the standard software tools, only for PRIMOS (the operating system of Prime computers -- actually, quite an interesting architecture, based on segments and rings ala Multics).

I was asked to write up the basic math library -- they didn't want to call the underlying Prime library for copyright reasons. I was asked because I was really, really good with the assembly language on the systems (having written a Pascal compiler and OS in the assembly language in the previous couple of years). So, I checked out some texts and wrote up some fast libraries and the test routines that were in the books. All looked good.

However, being the cautious type, I wanted to check that my code was indeed correct. I wanted an independent check. So, I asked around,

and found the Cody & Waite book. I coded all the tests, ran them against my library, and found one or two spots where I had not quite reduced arguments correctly. I fixed them until they passed both my original tests and the Cody & Waite tests. In the succeeding years, I never heard about any problems.

As a matter of curiosity, I ran the tests against the native OS library shipped with the Fortran compiler. I was aghast at the results! In some cases, the results were of the wrong sign and magnitude, didn't return errors for input out of range, and often lost about 60 out of 64 bits of precision! I wrote this up as a tech report (GT/ICS 83/09), and it was distributed to Prime and the Prime User's group, as well as included with the GT-WT distribution. I got mail from dozens of chagrined users of Prime systems who discovered errors in their systems because they had accepted the output of the math libraries -- including some astrophysicists who had to withdraw a paper claiming a better approximation of some constant, and a team of engineers who had been designing a nuclear reactor containment vessel using one of those systems!

A few years later, as a post doc, I pulled out the routines and got a grad student to help me rerun the experiments on several other systems we had around the lab at Georgia Tech. The result was issued as a tech report, Spafford, E.H.; Flaspohler, J.C.: A Report on the Accuracy of Some Floating-Point Math Functions on Selected Computers. Georgia Institute of Technology, Technical Report GIT-SERC-86/02, GIT-ICS-85/06, and then later published in ;Login: (the Usenix newsletter). The 14 systems we tested for our report included Vaxen running 4.2 BSD, a Pyramid 90x, an AT&T 3B20S, an AT&T

7300, a
Sun 2, a Ridge, a Cyber and a Masscomp -- each with its own OS
and
support system. I can't find a copy of the report still on the
WWW
anywhere, but in short, the results were that NONE of the systems
tested passed all the tests, and several produced results that
were
as far wrong as on the Prime system tested a few years earlier.
These were systems used regularly by engineering firms,
scientists,
NASA, the NRC, and more. Very scary results.

Today, we have people downloading code from the net and running
it,
integrating it into their mission-critical systems. The code is
produced without design, without formal testing, and by people
without adequate training to even understand there might be
problems. The focus everyone seems to have is on buffer
overflows,
but those are merely one symptom of sloppy software production.
There are lots of places where assumptions about the underlying
correctness of the system can be proven horribly wrong in
practice...as long-time RISKS readers understand.

Last time I checked, Cody & Waite was out of print, and an online
auction site had copies for over \$200 apiece.

I wonder how current-day systems would fare against these tests?
Given Bart Miller's experience with his "fuzz" testing over the
last
two decades, I wouldn't want to bet that current math libraries
work
correctly.

✉ **Re: Flat train wheels (Ladkin, [RISKS-24.51](#), Crepin-Leblond, [R-24.52](#))**

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>

Fri, 22 Dec 2006 07:58:27 +0100

I asked my railway-engineer colleague, Oliver Lemke, whether this phenomenon was known in Germany. Oliver noted that it has been known for thirty-plus years, ever since the introduction of the ET 420 EMUs for the Munich Olympics in 1972. The 420 series was the first with only disk brakes.

Some locomotive series, for example the 101 series which has been used to haul intercity passenger trains since 1996, are outfitted with "cleaning brakes" (German: "Putzbremsen"), which don't have any braking effect but clean any film from the wheels. The cleaning brakes operate automatically every couple of kilometers or so. They were installed, not because of braking problems, but because of problems starting and accelerating from a stop with heavy loads under conditions of poor adhesion.

Peter B. Ladkin, Causalis Limited and University of Bielefeld
www.causalis.com www.rvs.uni-bielefeld.de

✉ E-mail me at xx at yy dot zz

<Dan Jacobson <jidanni@jidanni.org>>

Thu, 28 Dec 2006 23:48:54 +0800

Why do I, the non-spam fearing jidanni@jidanni.org, find myself needing to say "jidanni at jidanni dot org" more and more these days?

No, not to protect from spam, but to protect from the spam protectors!

More and more well meaning news and mailing list software "protects" the addresses of spam fearers and non-fearers alike.

So if I want to ensure my e-mail address gets through unscathed, I must add the aforementioned hiccups, lest potential respondents be forced to enter some "click to reply" sign-up nightmare.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 54

Friday 19 January 2007

Contents

- [The problem of abstractions, or the lack thereof](#)
[Paul Robinson](#)
- [There's more to worry about than math libraries](#)
[Paul Robinson](#)
- [Mars Global Surveyor failure due to human error?](#)
[Al Stangenberger](#)
- [Unexpected changes](#)
[Andrew Koenig](#)
- [Cell phone in man's pocket sets him on fire](#)
[Mark Brader](#)
- [Excel Date Bug](#)
[Al Macintyre](#)
- [Travel to US to need all 10 fingerprints, credit and e-mail checks](#)
[Peter Mellor](#)
- [Another insecure login](#)
[Paul D.Smith](#)
- [Electronic flash, capacitors, and nerdy adolescents](#)
[Daniel P.B. Smith](#)

- [Re: Digital cameras converted to weapons](#)
[Sidney Markowitz](#) [Mark Brader](#)
 - [EVT 2007: Electronic Voting Technology workshop](#)
[David Wagner](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ The problem of abstractions, or the lack thereof

<Paul Robinson <paul@paul-robinson.us>>

Tue, 09 Jan 2007 23:33:53 -0500

I believe one of our biggest problems in the development of computer programs is the lack of adequate abstractions to be able to describe software in such a way as to reduce the amount of grunt work needed in the development of applications. We have not-very good tools and poor languages to describe what we want to accomplish. Plus, the people developing software are often not well trained, and the concepts are difficult, and often the customer doesn't even know what he wants, and may not even know how to articulate what he wants.

And even if he knows, and knows how to tell what he wants, he may not know how to get the developers on-line to understand his vision. (Every writer who has ever sold a book to Hollywood and saw the resulting movie, complains about how the screenwriter and director "botched" the translation and "bastardized" his or her story, so the idea of "concept" not equaling "implementation" isn't new.)

The point which can be made as far as software is concerned is that the higher the level of abstraction the greater the productivity the person is capable of producing. A programmer in a language like Cobol is going to be two to three times as productive as one in assembly language. A software designer using a system like, say, Ruby on Rails might be able to do ten times as much work as someone writing an application using, say, C or C++, presuming the target task is the same. I am using this as an example, I do not know if something like Ruby on Rails actually can give a full order of magnitude increase in productivity. But I wouldn't be surprised.

The only problem is that if you take abstraction to its ultimate conclusion, you get a language like APL which, except for some niche applications, failed dismally because it became too difficult to work with. But you could do some amazing things with it. The "big thing" in APL was to write a "one liner," an attempt to write a complete working application in one line of code. And I have seen some unbelievable stuff done with it. Things that conceivably might take dozens or hundreds of lines of code in a lesser programming language really could be done in *one line* of APL. I've seen it done. It kind of convinced me I'd never be able to do that kind of work, I don't have the background.

But to have that kind of capability requires a really powerful programming language, and/or excellent subroutine libraries to support it. As well as good people to write code using that language. It is often said

of APL that
it is a "write only" language in that some people would develop
cute tricks
but if you ever had to do maintenance it would be simpler and
easier to
start over.

But if you are even just competent in APL, the level of
abstraction of the
language is so high that your productivity will easily be at
least an order
of magnitude - maybe even two orders - higher than someone of
the same
capability working in any other programming language. And a real
"superstar"
could do things that might not even be possible even in a
considerably
longer period of time in anything else.

Some people have said similar things about Lisp and the increase
in
productivity they have seen from that as well. And I think the
point is
well taken: better tools to increase abstraction increase the
productivity
of programmers the same way - and for the same reason - power
tools increase
the productivity of carpenters. They allow them to do more in
the same
amount of time.

Our minds determine the tools we have. And the tools we have,
which
basically consist, as I have stated, of not-very-good code
editors, poor
programming languages, and inadequate run-time support, don't
make it
surprising that we have such problems in the development of
software. But
people are thinking about ways of improving it.

There is a guy named Louis Savain who has been doing some work
from

time-to-time on his idea: the creation of software modules using the concept of a hardware abstraction, limiting the number of interactions and cross-actions by limiting how side effects can occur. He was of the opinion that he had a great system for reducing error, increasing productivity and reliability of software. I pointed out to him that what he has is an *idea*. Unless and until he actually has something implemented all he has is a promise which may be useful but is at this time unproven.

Basically he wants to create for software what the transistor and the printed circuit did for electronics; to allow the fabrication of complicated components of extremely high reliability by limiting how one software module can communicate with another to rigidly defined interfaces. If I understand his proposals, what he wants to do is develop software visually in terms of components, and "wire" the components together. Hardware has rigidly defined interactions and race conditions can't occur because asynchronous operations are not possible. Except for the bootstrap of the machine, he would eliminate all software as we know it, even the operating system would work the same way, as modules with defined inputs and defined outputs and explicit interconnections between them. He may well be right in this point. Personally I believe he has some wonderful ideas and if he isn't right he's very close. But right now, that's all he has, ideas.

Almost two years ago I wrote an article for comp.risks (Vol. 23 No. 73, Item 5, 20 February 2005, "In the Matter of Component Architecture"),

in which I
stated that I felt one of the things we need is more work on
making software
packages to be more component based as opposed to mostly custom
development
from scratch almost every time.

An example I gave was on the comparison between buying a kitchen
makeover
and a maintenance change to a software package. With a kitchen,
you can
generally buy off-the-shelf components and have an almost exact
estimate of
the complexity, the time to finish and the cost. And everything
will fit
together and work right the first time. What we generally have
in the
software industry is a situation where the contractor will mill
the trees,
plane the lumber, forge the fasteners from the ore he will dig
up and smelt,
and build everything from scratch. Which is why they can't give
you a firm
estimate on delivery, or cost, or even guarantee that it will
work right
once it is constructed.

In short, we get away with the great kind of racket in our
business that no
one would tolerate from a Taiwanese manufacturer of toasters!

I got a number of comments explaining in their opinion why I was
wrong.
Most of them not only didn't get the analogy, they didn't
realize that most
of their comments reinforced my points.

One said the costs were different. Well, let's see, if you have
a "bet the
company" software package - let's say the checking account
program for
reconciling accounts run by a bank - which, with the original
purchase price

or with the original development, and all the subsequent modifications, has cost the bank upwards of five million dollars over the last twenty years, spending, say, US\$100,000 to do some upgrades to the system is the equivalent of spending \$10,000 on a \$500,000 house. It's in line with other real world examples. Or perhaps it points out we're spending a lot less money for what we are able to accomplish; while you can certainly get a fairly good selection of cabinets in Home Depot or Lowes for \$10,000, it's not a lot of money relative to the capital costs previously expended.

And that's what it comes down to is money. Software can do, for relatively low amounts of money relative to other costs, some really valuable things for a lot less money. Automation enables one to drastically scale up operations in capacity by a huge factor. Put up a bank building and have savings accounts and you can handle a few dozen customers per day. Which is what they did perhaps 150 years ago. Offer checking accounts and your customers can handle dozens of transactions a month with maybe one person to do the bookkeeping. And that's about as far as you can go without technology. So once the telephone comes around you can do a little more. Even if you offer multiple branches it's still limited to office hours. So as technology improves it's possible to do more things, like handle checks automatically so you don't have to keep hiring more people to do bookkeeping, as well as it being more accurate. Offer ATM access and customers can get to their money 24 hours a day. Network ATMs

and now your customers can get to their money from a million locations. Offer Touch-Tone access and they can check their balance and do account transfers "from over 650,000,000 convenient locations." But unless you want to hire thousands of people to handle around the clock to handle the transactions, you need computer software to do it. Now, that \$5,000,000 software program your bank which it started to run its checking account now functions to handle inquiries by telephone, and Internet, and withdrawals by local ATM and network ATM and transactions using a check card over a credit network, and automated deposits from the customer's employer.

Think that it's possible to do all that, in reasonable amounts of time, with human beings in the loop? And not only that, they can do all these things for less money than it costs for the people involved. So software provides tremendous benefits relative to the cost of its production. And if it can be mass marketed it can be extremely lucrative.

As it stands now, things are "good enough" to get by and even with all the failures we have, there is so much value for such little costs that we keep stumbling along. Improvements can radically increase that value we can squeeze out of software which is why there is so much interest, but there is so much value now that even with the primitive tools and capabilities we have now, we can do some spectacular things.

The lessons of history teach us - if they teach us anything - that

nobody learns the lessons that history teaches us

✶ There's more to worry about than math libraries

<Paul Robinson <paul@paul-robinson.us>>

Wed, 10 Jan 2007 18:35:47 -0500

Some people here have posted articles regarding errors in the math libraries of some systems. But there is another problem; in some cases, there *are* no math libraries, so you might not even know if there is wrong and even if you did notice it was wrong, you might not even know how to correct it.

Now, the following comments on the content of compilers currently all apply only to open-source compilers since closed-source ones generally don't even let you see what's going on in the run-time code modules.

I read sources of program compilers both as a learning exercise and to understand how compilers work. (I've written about 4 (small) compilers and one (tiny) operating system, and I'm currently working on a translator adequate to translate Cobol so that I can implement something which I think has not been done before, a self-hosting Cobol compiler (a compiler which is self-hosting means the compiler and the source language of the compiler are the same.))

One of the things that has bothered me in all of the compilers I've seen, even the ones that are designed to support multiple targets, is

their use of
the built in mathematical functions of the current 586 class
microprocessor.
This means that, when one wants, say, a square root, instead of
the run-time
library doing a calculation for square root approximation loop,
the compiler
generates instructions inline to put a value into a floating
point register
and issues the square root machine instruction, and retrieves
the result
from a register, and returns the result for processing. (Or, in
some cases
this is the entire square root subroutine; get the value, pass
it to the
square root machine instruction, and return the value.) I'm not
picking on
square root specifically, I can include some of the other
transcendentals
such as sine, cosine, tan etc.

Okay, I do understand that it is done to provide a speed
advantage, because,
obviously, a hardware-performed operation is going to be
considerably faster
than any software implementation. But it does cause two
problems: first, it
doesn't provide a reference implementation for the particular
mathematical
function other than use of the hardware. Second, the
implementation is
non-portable. Even though the compiler is often written for
multiple
machines or should be easy to port, there is nothing available
to use for
that mathematical function if the compiler is to be implemented
on another
machine.

It also means if someone develops a better algorithm for that
function, if
that function is done inline, instead of being able to
substitute a new

routine one has to find where the inlining of square root is done and change it back to what it should have been in the first place: a procedure call,

This also, to some degree, causes a "loss of institutional memory" for lack of a better term; since nobody has seen code on how to perform the mathematical function, nobody knows how it works, nor is there much information on how the function is performed, thus there isn't much there for someone to look at how it is done and develop improvements.

What I would really like to see - and have seen in some better compiler applications - is where the function has been implemented, even if crudely, and the implementation is still present but has been disabled in favor of the equivalent but faster machine function. Thus, especially where the function is implemented in the high-level language, it is possible to provide functionality when re-implementing a language compiler on another system.

✶ Mars Global Surveyor failure due to human error?

<Al Stangenberger <forags@nature.berkeley.edu>>

Thu, 11 Jan 2007 09:37:52 -0800

NASA is investigating whether incorrect software commands may have doomed the Mars Global Surveyor spacecraft, which abruptly fell silent in June 2006 after a decade of meticulously mapping the Red Planet. This is

is just one of several theories that may explain the probe's failure. NASA announced the formation of an internal review board to investigate why the Global Surveyor lost contact with controllers during a routine adjustment of its solar array. [Source: *San Francisco Examiner*, PGN-ed]
http://www.examiner.com/a-501893~Human_Error_May_Have_Doomed_Mars_Probe.html
[Also noted by Walter Schilling:]
<http://www.spaceref.com/news/viewnews.html?id=1185>.

⚡ Unexpected changes

<"Andrew Koenig" <ark@acm.org>>
Thu, 4 Jan 2007 13:20:19 -0500

Today I logged into my Vanguard account (In case you're unfamiliar with it, Vanguard is one of the larger financial companies in the USA, and offers mutual funds, brokerage, and cash-management services). I was greeted by the following message:

The Accounts & Activity area of our site is currently reflecting brokerage account holding information from Tuesday, January 2, 2007, instead of Wednesday, January 3, 2007. We apologize for any inconvenience and are working to correct this situation as soon as possible.

I am guessing that their software was unable to cope with the markets being closed on January 2 for President Ford's funeral. Indeed, last night they

displayed the balance of one of my mutual funds, held through their brokerage service, as zero dollars. They had the right number of shares, but the price was \$0.00 per share. I am guessing that their software expected to see a price quote because it thought the markets were open, but didn't get one; so it substituted zero.

Usually Vanguard is pretty good about systems stuff, but no one's perfect. I imagine that their programmers are pretty busy right now...

⚡ Cell phone in man's pocket sets him on fire

<msb@vex.net (Mark Brader)>
Tue, 16 Jan 2007 13:41:58 -0500 (EST)

(Search Google News for "luis picaso".)

⚡ Excel Date Bug

<Al Mac <macwheel99@sige.com.net>>
Wed, 10 Jan 2007 11:42:35 -0600

Here is link to article explaining what they label as a well known bug in Excel: It does not do leap year math correctly.

<http://www.itjungle.com/fhg/fhg011007-story01.html>

✈️ Travel to US to need all 10 fingerprints, credit and e-mail checks

<MellorPeter@aol.com>

Sun, 7 Jan 2007 18:22:25 EST

This was reported today in the UK Sunday newspaper The Observer and in AOL

News (and probably in lots of other places). See:

<http://observer.guardian.co.uk/world/story/0,,1984496,00.html>

<http://news.aol.co.uk/us-to-hold-britons-fingerprints/article/20070107151109990002>

The headlines mention "Britons", but the measures apply to all EU countries, Japan, Australia and New Zealand.

The scheme will be tried out in 10 major airports from this summer and is planned to be in use in all airports and seaports by the end of 2008.

The main points are that, for travelers entering the US:

- all 10 fingerprints will be taken, which is compatible with the FBI database (only two prints are currently taken);
- the prints will be retained indefinitely and with no restriction on their international use or sharing with other agencies;
- inspection of credit card and email accounts (already practised) will be strengthened.

With regard to the last point, the Observer article states:

"Britons already have their credit card details and email accounts inspected by the American authorities following a deal between the EU and the Department of Homeland Security. Now passengers face having all their credit

card transactions traced when using one to book a flight. And travelers giving an email address to an airline will be open to having all messages they send and receive from that address scrutinised.

The demands were disclosed in 'undertakings' given by the Department of Homeland Security to the EU and published by the Department for Transport after a request under the freedom of information legislation."

It is not made clear exactly what will be inspected: all transactions or messages after the date of booking, any previous transactions or messages?

Will the DHS be concerned about my credit card or e-mail account if I buy a ticket from a travel agent for cash? This could be the end of on-line booking of flights to the US. (Of course, no international terrorist would dream of using a forged card or setting up an e-mail account under a pseudonym.)

The 'invasion of privacy' issues are pretty obvious and civil liberties groups are predictably jumping up and down.

Peter Mellor; Mobile: 07914 045072; email: MellorPeter@aol.com

Telephone and Fax: +44 (0)20 8459 7669

Another insecure login

<"Paul D.Smith" <paul_d_smith@hotmail.com>>

Wed, 3 Jan 2007 10:29:59 -0000

Readers might like to beware of <http://www.genesreunited.co.uk>. This is a legitimate, and very useful, genealogy website that is sadly let down by its login, which uses an insecure HTTP page to transmit user account name and password in the clear.

I have contacted the support contacts pointing out the security implications but, surprise, their support team don't seem to understand the problem and I've failed to get through to anyone who will acknowledge that a problem exists.

Since this site requires a small payment before all services are available, I do wonder what comeback I have should someone sniff my account details and then trash my family tree information carefully stored there - or worse start doing something that attracts the attentions of "those who watch the web" (OK, so I'm being a little paranoid but I program computers so it's in my nature!).

FOLLOW-UP Date: Wed, 3 Jan 2007 17:21:21 -0000

I just noticed the following message on the "My Details" page - the one where the name and password may be altered...

"From this page you can manage your details on Genes Reunited. This page is password protected - your login and contact details cannot be seen by anyone else."

Using Wireshark I quickly confirmed that this is nonsense and all passwords are sent in the clear. Naughtily, the page also has a padlock

next to "This
page is password protected" to confuse the unwary.

⚡ **Electronic flash, capacitors, and nerdy adolescents**

<"Daniel P. B. Smith" <usenet2006@dpbsmith.com>>
Sat, 23 Dec 2006 06:46:19 -0500

My reaction to Mark Brader's story, about teenagers making
electric shock
weapons from disposable digital cameras, was "I'm surprised that
it took so
long."

By the late 1950s, electronic flash units were popular among not-
even-
very-serious amateur photographers. The little camera shop in my
town sold
many models. By the 1960s relatively compact units that snapped
into the
flash shoe on atop most cameras were common. And, yes, consumer
photo
magazines like Popular Photography warned of the dangers of the
capacitors
inside. The size and power of these flash units was much larger
than those
of the tiny ones built into cameras today, and I suspect that
under some
conditions they could well have been lethal.

And the long-drawn-out suspense as the squeal of the transformer
rose and
pitch, and ready light began to flash faster and faster
certainly gave an
idea of immense power being concentrated. Like the slow climb at
the start
of a rollercoaster ride.

In those days a friend of mine and I were doing a lot of the

sorts of things
nerdy adolescent males do--breaking open radios and
transistors and radio
tubes and almost anything we could break open. To see what was
inside. And
repurpose and play with the parts. We also liked to toss
charged capacitors
at each other, hoping the victim would try to catch them. And we
liked to
shock each other with the hand-crank generators you could at the
time get
from surplus electronics houses.

Either, (a) I had enough sense of self-preservation not to try
anything
funny with my electronic flash unit, or (b) I wasn't sure how I
was going to
explain to my parents why I had switched back to using
flashbulbs, so I
never actually made anything weapon-like out of my electronic
flash. But
with regard to the possibility, teenagers have had the means,
motive, and
opportunity for half a century.

(Hypothetically, there might have been the potential to do
creative
things with flashBULBS, too. Cheap little packages of
pyrotechnic materials,
designed to ignite reliably and instantaneously from a small
amount of
electricity...)

⚡ **Re: Digital cameras converted to weapons ([RISKS-24.52](#))**

<Sidney Markowitz <sidney@sidney.com>>
Sat, 23 Dec 2006 12:52:07 +1300

The article on converting a camera to a "taser" incorrectly talked about disposable digital cameras, which do not currently exist. In fact, the conversion is done using any inexpensive disposable camera with a flash unit. The xenon flash bulb requires a 1000 to 10000 volt trigger pulse to fire, supplied at low current from a typically 300 volt capacitor discharged through a trigger coil. Replace the bulb with a couple of wires and you can use it to give someone a painful shock just by taking a picture while touching them with the wires. It is not nearly as powerful as one from a real stun gun such as a taser, which delivers on the order of 100,000 volts or more.

The news that you can make a painful device from a cheap camera may be shocking to some, but it is not much different and less dangerous than many homemade weapons that teens have been known to make from common materials such bicycle inner tubes or car radio aerials. A real risk may be that someone may not take seriously the potential dangers of the shock. It may usually be a painful but harmless prank, but with the wrong victim or the wrong circumstances could cause death.

⚡ Re: Digital cameras converted to weapons (Brader, [RISKS-24.52](#))

<msb@vex.net (Mark Brader)>

Fri, 22 Dec 2006 11:20:21 -0500 (EST)

I wrote:

> weapons ... produced by teenagers from disposable digital cameras!

However, I should not have said "digital" there (nor in the subject line).

Nor should I have confused Brentwood with Brentford a couple of issues back.

Sorry about that (slaps self!), and thanks to Chris Drewe and Ed Davies for catching my slips.

[This is what I get for trying to be helpful instead of just sending the URLs and letting PGN do the PGning! Sigh.]

[Nevertheless, it should be obvious that PGN appreciates people who take

the effort to abstract/summarize and comment rather than just sending the

bare URL or the entire copyrighted text. PGN]

✶ EVT 2007: Electronic Voting Technology workshop

<David Wagner <daw@cs.berkeley.edu>>

Thu, 18 Jan 2007 12:26:35 -0800 (PST)

The 2007 USENIX/ACCURATE Electronic Voting Technology workshop (EVT 2007)

will be on 6 Aug 2007. The call for papers is available here:

<http://www.usenix.org/events/evt07/cfp/>

Paper submissions are due 22 Apr 2007. Please encourage your colleagues,

students, etc. to send us their best papers.

[The papers from the first workshop, EVT 2006, in Vancouver, are online:

<http://usenix.rutgers.edu/library/06evt/tech/index.html>

It was an outstanding workshop. The community of awareness on the risks of electronic voting systems has grown enormously, since then.

I hope that some of you will be able to submit papers to EVT 2007. 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

Search RISKS using [swish-e](#)

Volume 24: Issue 55

Saturday 3 February 2007

Contents

- [Super Bowl site hacked, seeded with exploits](#)
[EEkid](#)
- [Ed Felten: AACS Decryption Code Released](#)
[Monty Solomon](#)
- [/Mis/using a laptop to compute take-off parameters on a B747-400](#)
[Philippe Jumelle](#)
- [Customer was sent 75000 bank statements](#)
[Martyn Thomas](#)
- [Another example of bad software](#)
[Avi Rubin](#)
- [Windows Vista voice vulnerability](#)
[Joe Loughry](#)
- [Daylight savings time mess looms](#)
[Lauren Weinstein](#)
- [Massachusetts Attorney General sees card fraud close up](#)
[Mark Lutton](#)
- [Canadian coins containing tiny transmitters](#)
[Mark](#)

- [StopBadware blacklists a cartoon book site](#)
[Jim Youll](#)
 - [Doesn't sound like a laser pointer to me...](#)
[Paul Saffo](#)
 - [Square roots](#)
[Andrew Koenig](#)
 - [Risks of one's complement arithmetic?](#)
[Daniel P.B. Smith](#)
 - [Re: Excel Date Bug](#)
[Steve Wildstrom](#)
 - [Re: Cell phone in man's pocket sets him on fire](#)
[Lauren Weinstein](#)
 - [REVIEW: "Security Governance", Fred Cohen](#)
[Rob Slade](#)
 - [REVIEW: "Knowledge Power: Intellectual Property, Information and Privacy", Renee Marlin-Bennett](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Super Bowl site hacked, seeded with exploits (via Dave Farber's IP)

<EEkid@aol.com>

February 2, 2007 5:41:10 PM EST

A visitor to the site with an unpatched Windows machine will connect to a remote server registered to a nameserver in China and download a Trojan keylogger/backdoor that gives the attacker full access to the compromised computer. " <http://blogs.zdnet.com/security/?p=15>

✶ Ed Felten: AACS Decryption Code Released

<Monty Solomon <monty@roscom.com>>

Wed, 24 Jan 2007 22:13:14 -0500

AACS Decryption Code Released

Monday January 8, 2007 by Ed Felten

Decryption software for AACS, the scheme used to encrypt content on both next-gen DVD systems (HD-DVD and Blu-ray), was released recently by an anonymous programmer called Muslix. His software, called BackupHDDVD, is now available online. As shipped, it can decrypt HD-DVDs (according to its author), but it could easily be adapted to decrypt Blu-ray discs.

Commentary has been all over the map, with some calling this a non-event and others seeing the death of AACS. Alex Halderman and I have been thinking about this question, and we believe the right view is that the software isn't a big deal by itself, but it is the first step in the meltdown of AACS. We'll explain why in a series of blog posts over the next several days.

Today I'll explain how the existing technology works: how AACS encrypts the content on a disc, and what the BackupHDDVD software does. ... <http://www.freedom-to-tinker.com/?p=1104>

[See Ed's blog for many other RISKS-relevant items on AACS and more. PGN]

✈/Mis/using a laptop to compute take-off parameters on a B747-400

<"Philippe Jumelle" <pjumelle@gmail.com>>

Thu, 1 Feb 2007 11:36:47 +0100

I leave it to aviation experts RISKS readers to elaborate on the following:

A French Boeing 747-400 fully packed with passengers bound to the Caribbean suffered a "tail strike" incident in December 2006.

The "Bureau d'Enquêtes et d'Analyses" issued a report (<http://www.bea-fr.org/docspa/2006/f-ov061210/pdf/f-ov061210.pdf>, available in French only) that explains how a misused "Boeing Laptop Tool" (laptop PC) was involved in this incident:

2 BLTs are available in the aircraft. They are used to compute important take-off parameters including Vr (rotation speed) and EPR (engine thrust).

One of them had an empty battery. The other one was switched off mistakenly during the flight preparation procedure. After restart, wrong parameters were entered by the crew member and a mix-up between ZFW (Zero Fuel Weight) and TOW (Take-Off Weight) occurred, resulting in incorrect flight parameters displayed on the BLT and entered in the Flight Management System.

Fortunately, the crew noticed that parameters were wrong while attempting take-off and took appropriate action, resulting however in this "tail strike". As a consequence, the aircraft was visually inspected by a fighter for damages and landed safely at the departure airport after dumping fuel.

The airline issued recommendations to the crews so that they make sure that BLTs are properly plugged into AC power while the aircraft is on the ground (flat battery, hibernation risk) and described cross-check procedures avoiding over-reliance in BLT output.

Customer was sent 75000 bank statements

<"Martyn Thomas" <martyn@thomas-associates.co.uk>>
Mon, 29 Jan 2007 19:21:23 -0000

http://news.bbc.co.uk/1/hi/scotland/north_east/6310633.stm

An Aberdeen woman who asked for her bank statement was sent those of 75,000 other customers. Stephanie McLaughlan, 22, was shocked when Halifax Bank of Scotland (HBOS) sent her the unexpected financial details by mistake. Ms McLaughlan received several large packages in the post and said she was concerned it could happen. HBOS apologised and said it was carrying out an investigation into the "serious" but "isolated" incident.

HBOS said in a statement: "We are treating this matter very seriously and are investigating in full. "This is a very specific, isolated incident and we will take steps to ensure there is no security issue for customers as a result of this matter. "We apologise for any concern this has caused customers."

[Also noted by Bernhard Riedel: ``I have real trouble trying to imagine

how many 'pilot errors' it requires for such a report to be mailed to an ordinary customer. Banks should be more accountable than that.' ' PGN]

⚡ Another example of bad software

<Avi Rubin <rubin@jhu.edu>>
Tue, 30 Jan 2007 07:25:56 -0500

Bad Software All Around
<http://avi-rubin.blogspot.com/>

Earlier this week, I took a train up to NYC to give a talk to some potential [ISE](http://securityevaluators.com) customers on Wall St. A collection of Chief Information Security Officers and other executives from financial firms. I was asked to speak about software security, and two things happened on this trip that put to rest any doubt that the current state of software security and network security is dismal. I didn't doubt it, but I thought it was particularly humorous that these happened on a trip whose purpose was to give this particular talk.

I arrived at my hotel about an hour before I was scheduled to speak. Since the hotel was only a couple of blocks from Wall St., I figured that I had time to go online and read my email. I opened up my laptop in my room and saw that there was a WiFi base station whose SSID was "Exchange" (which was the name of my hotel) along with several other available base

stations. So,
I connected to my hotel's access point. I had full bars, so the connection
was strong, but I was unable to reach my email server. I had a look at the
IP address assigned to me by the network and noticed that it was a factory
default address that was probably not what the hotel was using. So, I called
the front desk, and I told the woman who had just checked me in that I was
having a problem with the wireless network. It seemed that I was not getting
a valid IP address. She said something about their street address, and I
realized that while this nice lady was very good at checking me into my
room, she was not going to be the best tech support person I had ever had.

I explained to the woman that I was able to connect to the wireless network,
but that I was unable to read my email because the network was not
working. She understood that and said, "Yes, this happens all the time. I
will just reboot the thingy. Give it a few minutes and try again." That
sounded like a reasonable solution. Meanwhile, I tried the other wireless
networks, and none of them would allow a connection without a password. I
chalked this up to progress.

Several minutes later, I reconnected to the Exchange network, and I was
assigned what looked like a normal NATed IP address. But, I was still unable
to connect anywhere. So, I opened up a browser window to see if I needed to
log in. What I saw surprised me at first. It looked like some kind of menu
console for managing an appliance. I clicked around and realized

that I had the ability to configure routing and firewall rules. In fact, I was logged into the hotel's router - the "thingy" if you will. I smiled to myself at the thought of what I could do if I wanted to, but I quit out of that and was able to access the Internet. The connection was pretty slow, and I chuckled at the thought of getting back into the administration console to filter out the other users in the hotel. Of course, I decided against that.

Unbelievable!

But, it gets better.

When I arrived back at Baltimore Penn Station, I left the train and walked to my car. I drove up 2 levels in the parking garage, and I arrived at the exit gate. This parking garage installed an automated system where you use a credit card to get in when you arrive, and if you use the same credit card when you leave, you don't need to take a ticket, and it charges that card and lets you out. At least that's the theory. It didn't work that way on this trip. As I approached the exit, I saw that there were two lanes open for exiting, and that the car in front of me had pulled into one of them. So, went to the other one and inserted my credit card. On my mind was my daughter's school play, which started in about an hour. I had time to grab a quick sandwich and then head to her school. I had planned my trip so that I could be back in time to see her perform.

After about a minute, it seemed odd to me that my credit card

had not come out yet. The machine said that it was validating ticket data. But, I had not inserted a ticket. So, I pressed the intercom button, and an attendant asked if she could help me. I told her that I put my credit card in a while ago, and that I wanted to pay and leave. The gentleman in the truck in the other lane yelled to me that he was in the same boat, so I told the woman that neither one of us could leave. She asked us to hold on a second, and in about another minute a woman in a parking attendant uniform appeared. She told me that it might be that the other gentleman and myself inserted our credit cards at the exact same time in the two different machines. I agreed that this was indeed possible. In the meantime, I rather long line of cars had formed behind us.

The parking attendant backed up all of the cars and suggested that I back up about one car length, and that the other gentleman do the same. Then, she suggested that I drive back up to the machine, which I did. My credit card came out, but she said I had to reinsert it. I did, and it said that it was validating ticket data. The attendant said, "oh no." That didn't sound good. I asked what the problem was. She said that every once in a while, when two people insert their credit cards at the exact same time, it crashes their whole system. We did the back up thing again to retrieve our cards. Since the other guy was first, she went and processed his payment manually. That took about 3 minutes. Then, she took my credit card and went

to do mine. In the meantime, another car behind me drove into the other lane, which was now available and inserted his card. The system did not respond. It was hosed. A few minutes later, she came back and gave me my credit card and receipt and opened the gate so that I could exit. The line of cars was now very long, and she said she would have to do them all by hand until a technician could come. I have no idea where this technician was coming from, but I was glad to be on my way. I got that sandwich, but because of my delay, I had to eat it in the car on the way to my daughter's play.

What kind of software design results in this kind of crash? The answer is pretty clear to anyone who has worked with software. While they may have tested the system exhaustively, they probably did not test the possibility of putting credit cards in two different machines at the exact same time. Which brings me back (as usual on this blog) to voting machines. They may be tested and tested and certified and verified and validated. But, if on Election Day something unusual happens, a scenario that was not anticipated, something might go very wrong. And, if there is no tangible, physical record of the votes that were cast on the machine, then votes might be lost in an unrecoverable way.

Given what I've seen about voting system standards and voting system testing labs, I would bet money that the parking garage system at Baltimore Penn Station was tested more extensively before it was deployed than

the Diebold
voting machines that we use in Maryland.

Avi Rubin, Johns Hopkins University, Computer Science, Tech.Dir.
Information
Security Institute 1-410-516-8177 <http://www.cs.jhu.edu/~rubin/>
rubin@jhu.edu

Windows Vista voice vulnerability

<Joe Loughry <joe.loughry@lmco.com>>
Thu, 01 Feb 2007 09:11:26 -0700

Here's a good one:

1. Microsoft Windows Vista comes with voice recognition installed and active by default.
2. Voice services has tons of security privileges, since it is a "local" service and therefore safe, right?
3. Playing a sound through the speakers on Vista requires almost no security privileges, since that's a harmless operation, right?
4. By playing a prerecorded file of spoken commands, an unprivileged process can execute arbitrary processes that get executed with elevated security privileges.

<http://isc.sans.org/diary.html?storyid=2148>

Microsoft promises to have a patch for this "real soon now."

⚡ Daylight savings time mess looms

<Lauren Weinstein <lauren@vortex.com>>

Wed, 31 Jan 2007 22:10:46 -0800 (PST)

When few people were paying attention in August 2005, Congress lengthened daylight saving time by four weeks in the name of energy efficiency. The change takes effect on 11 Mar 2007. It has angered airlines and creates many problems for automated systems that are preprogrammed to switch by the old schedule. [Source: Charles Babington, Clocks' Early Spring Forward May Bring About a Few Falls *The Washington Post*, 1 Feb 2007; PGN-ed]

[This is another iteration on an old RISKS topic. Each year brings

more new items. Stay tuned for this one in five more weeks! PGN]

⚡ Massachusetts Attorney General sees card fraud close up

<<Mark.Lutton@thomson.com>>

Sat, 20 Jan 2007 20:30:44 -0500

The Boston Globe story looks like the best coverage.

http://www.boston.com/news/local/massachusetts/articles/2007/01/19/just_seated_ag_nearly_gets_burned_by_fraud/

Boston Herald

<http://news.bostonherald.com/localRegional/view.bg?articleid=177931>

This story is not being reported outside of Boston. It has appeared only in the Boston newspapers and television stations. The new

Massachusetts

Attorney General, Martha Coakley, was the target of attempted credit card fraud a week before she was sworn into office. Coakley received a telephone message from Dell Computer asking to confirm whether she had ordered a \$1,200 computer to be shipped to an address in Texas. She had not. She quickly canceled the transaction and also closed her credit card account.

The Boston Globe: "As a prosecutor, however, Coakley said she couldn't help being frustrated that no one was going after the perpetrator. She doesn't know how someone obtained her credit cards number -- or how Dell found her phone number."

Or whether the call was really from Dell, I think. That must be one of those "unknowns we don't know we don't know."

If a state Attorney General is helpless against card fraud, what chance do the rest of us have?

Mark Lutton, Business Intelligence Services, a Thomson Business

Canadian coins containing tiny transmitters

<Mark - Syminet <mark@syminet.com>>

Mon, 22 Jan 2007 20:35:52 -0800

Canadian coins containing tiny transmitters have turned up in the pockets of at least three American defence contractors...

<http://www.cbc.ca/technology/story/2007/01/10/rfid-defence.html>

⚡ StopBadware blacklists a cartoon book site

<Jim Youll <jim@challengeandresponse.com>>

Fri, 12 Jan 2007 17:32:38 -0500

The (possible) risks of well-intentioned but (apparently) uncoordinated censorship

Who's watching the watchers? (StopBadware blacklists a cartoon book site)

Capefeare.com, described as "The Ultimate Life in Hell Website", is blacklisted in Google, which cites StopBadware.org as the source. However, StopBadware.org doesn't list the site in its database. I can't find anything wrong at the site and it seems to be legit (and popular). What's going on here, and who's watching the watchers? 11 Jan 2007

http://bbaadd.com/blog/2007/01/whos-watching-watchers-stopbadware_11.html

⚡ Doesn't sound like a laser pointer to me...

<Paul Saffo <paul@saffo.com>>

Sun, 21 Jan 2007 10:42:16 -0800

[perhaps it was a dermatology tool?]

Laser pointer causes Miracle Mile office fire [Associated Press, 21 Jan 2007]

A hand-held laser pointer caused a fire at a Miracle Mile high rise that caused \$200,000 in damage, a fire official said. The blaze at the 17-story office building at 6200 Wilshire Blvd. began just after 10 a.m. Saturday, said Los Angeles city fire spokesperson Brian Humphrey. The laser device had been laid on an examination table in a 12th floor dermatologist's office, Humphrey said. The device ignited surrounding furnishings, sparking the fire. The fire was extinguished by the building's sprinkler system, Humphrey said. Firefighters mopped up about 3 inches of water. There were no reports of injuries.

<http://www.mercurynews.com/mld/mercurynews/16513705.htm>

⚡ Square roots

<"Andrew Koenig" <ark@acm.org>>
Sat, 20 Jan 2007 11:37:30 -0500

Paul Robinson complains about compilers that use hardware square-root instructions instead of software-based math libraries.

I believe that in the specific case of square root, this complaint is misplaced on IEEE-754 compliant processors, because the IEEE 754 standard requires compliant processors to compute square roots accurately.

It is true that a processor whose manufacturer claims that it complies with the standard might not actually comply, either because of defects or design errors. However, that problem exists for more primitive instructions as well, as we saw with the Intel floating-point division bug. In such cases, the solution lies in testing the hardware, not in refusing to use it.

[Something like trying to fit square roots in a round-off?
PGN]

⚡ Risks of one's complement arithmetic? (Re: Lee, [RISKS-24.53](#))

<"Daniel P. B. Smith" <dpbsmithadhoc@dpbsmith.com>>

Sat, 30 Dec 2006 08:48:32 -0500

> the sudden energy of all the bits turning from 1 to 0 got
> coupled into
> that wire and caused the fault.

Well, maybe, but I have to wonder.

The PDP-1 was a one's complement machine with two arithmetically equivalent representations of zero. Most current machines are two's complement; the word with all bits set represents the arithmetical value -1. On the PDP-1, all bits set was "minus zero" and all bits clear was "plus zero."

The two values were equivalent when functioning as operands in arithmetic operations.

But there was also a special, designed-in feature, colloquially

referred to
as "minus-zero gronking." On arithmetic operations (and only on
arithmetic
operations) if the result of an operation was minus zero, it was
automatically changed to plus zero. I forget what the rationale
for this
was; presumably it was for convenience in testing whether
results equaled
zero.

But the two values ought to have displayed identically on the
screen, too.

Was this really an electronic error or was it an unexpected (and
poorly
understood) consequence of the PDP-1's intended functioning?

⚡ Re: Excel Date Bug ([RISKS-24.54](#))

<steve_wildstrom@wdc.exchange.businessweek.com>
Sun, 21 Jan 2007 12:08:35 -0500

It's hard for me to believe that any developer doesn't know
about the Excel
date problem, which has actually been around since Lotus 1-2-3.
The history
of the bug, as well as Microsoft's explanation for why fixing it
would cause
more problems than it would solve, is at
<http://support.microsoft.com/kb/214326/en-us>.

Steve Wildstrom, Technology & You Columnist, BusinessWeek
1200 G St. NW Suite 1100, Washington, DC 20005

⚡ Re: Cell phone in man's pocket sets him on fire (Brader, [RISKS-](#)

24.54)

<Lauren Weinstein <lauren@vortex.com>>

Fri, 19 Jan 2007 15:33:20 -0800

This story has already been debunked. Not true.

[I suppose the man de-bunked himself fairly quickly as well.
PGN]

REVIEW: "Security Governance", Fred Cohen

<Rob Slade <rMslade@shaw.ca>>

Wed, 31 Jan 2007 11:27:19 -0800

BKSECGOV.RVW 20061110

"Security Governance", Fred Cohen, 2005, 1-878109-37-5

%A Fred Cohen <http://all.net>

%C 572 Leona Dr, Livermore, CA 94550

%D 2005

%G 1-878109-37-5

%I Fred Cohen and Associates

%O 925-454-0171 all.net

%O [http://www.amazon.com/exec/obidos/ASIN/1878109375/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/1878109375/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/1878109375/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/1878109375/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/1878109375/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/1878109375/robsladesin03-20)

%O Audience a Tech 1 Writing 2 (see revfaq.htm for explanation)

%P 96 p.

%T "Security Governance: Business Operations, Risk Management,
and

Enterprise Security Architecture"

Most of the security frameworks available are in the form of a

checklist, so why shouldn't Cohen's CISO Toolkit (see also BKCISOGG.RVW for the "Governance Guidebook" and BKCISOHB.RVW for "The CISO Handbook") have one?

In fact, Cohen's version may be considerably easier to understand and use, particularly for those with a business, rather than a security, background. While most security frameworks are structured according to a taxonomy of security concepts, the checklist in "Security Governance" is based on business models and concepts. For example, the four major divisions are made on the basis of business functions and modelling, oversight, business risk management, and enterprise security management. Therefore, the businessperson working through the points will start with the familiar, and only later have to face items directly discussing security. (Even then, the security issues are those regarding the position and management of security within the organization.)

Regardless of other security frameworks that you may use, Cohen's checklist will be of value. While many items will have relations to details in other indices, the articles and entities in "Security Governance" address a number of issues that are not found in most security frameworks. Let's face it: regardless of the emphasis or perspective, security frameworks tend to follow the same general outline. Cohen's work is idiosyncratic--and, in this case, that's a useful characteristic.

Also, most security frameworks give you a checklist of about 135 items for roughly U\$150: Cohen gives you over 900 points for U\$49.00.

copyright Robert M. Slade, 2006 BKSECGOV.RVW 20061110
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>

REVIEW: "Knowledge Power: Intellectual Property, Information and Privacy", Renee Marlin-Bennett

<Rob Slade <rMslade@shaw.ca>>
Mon, 08 Jan 2007 13:31:27 -0800

BKKPIPIP.RVW 20061119

"Knowledge Power: Intellectual Property, Information and Privacy",

Renee Marlin-Bennett, 2004, 1-58826-281-2, U\$23.50

%A Renee Marlin-Bennett

%C 1800 30th St., Boulder, CO 80301

%D 2004

%G 1-58826-281-2

%I Lynne Rienner Publishers

%O U\$23.50 www.rienner.com

%O <http://www.amazon.com/exec/obidos/ASIN/1588262812/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/1588262812/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/1588262812/robsladesin03-20>

%O Audience i- Tech 1 Writing 1 (see revfaq.htm for explanation)

%P 273 p.

%T "Knowledge Power: Intellectual Property, Information and Privacy"

Chapter one examines the idea of intellectual property (IP). This analysis

could have been either prescriptive (what IP should be) or descriptive (what IP is, usually in terms of law), but instead it mostly opines prescriptively, and, when there is a need to take a stand, cravenly goes to what the legislation (generally from the United States) says. (There is some mention of international differences.) A link between privacy and IP is promised in one section, but not delivered. A historical overview of the development of IP is given in chapter two: when it gets to current definitions we are again presented with US law. Treaties and organizations attempting to bridge national differences in IP are listed in chapter three. Chapter four presents some examples of problem areas in IP, such as pharmaceutical patents and those on sections of the human genome.

A few philosophical views and theories of information are outlined in chapter five, followed by a discussion of information of various types and values. (The deliberation would have been more interesting if the types had been analyzed in light of the different theories.) Chapter six looks into the pros and cons of "ownership" and limitation of public types of data, such as that in regard to weather and geography. Similarly, chapter seven has the same type of discussion regarding information about people (much of it in relation to issues of surveillance.) Chapter eight has the same problems with the definition of the topic that most other works have had, which is possibly why the remaining examination seems unhelpful. There are numerous technical errors ("Magic Lantern" is **not** a virus) in chapter

nine's discussion of privacy breaches. Similarly, the deliberation on privacy protection technology, in chapter ten, is flawed. Chapter eleven finishes off with vague opining.

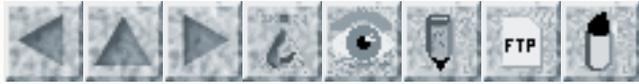
There are a number of other books that address the topic of privacy at the same superficial level, such as "Benjamin Franklin's Website" by Robert Ellis Smith (cf. BKBNFRWS.RVW), Simson Garfinkel's "Database Nation" (cf. BKDBSNTN.RVW), Peterson's "I Love the Internet But I want My Privacy Too" (cf. BKILIWMP.RVW), Cannon's "Privacy" (cf. BKPRVACY.RVW), and "The Privacy Papers" by Rebecca Herold (cf. BKPRVPAP.RVW). Then there are the superior works that define the field, like "Technology and Privacy: The New Landscape" by Agre and Rotenberg (cf. BKTCHPRV.RVW), 1997, Cady and McGregor's surprisingly good "Protect Your Digital Privacy" (cf. BKPYPDRV.RVW), "Internet and Online Privacy" by Frackman, Martin and Ray (cf. BKINONPR.RVW), Schneier and Banisar's entertaining and informative "Electronic Privacy Papers" (cf. BKELPRPA.RVW), and "Privacy on the Line" by Whitfield Diffie and Susan Landau (cf. BKPRIVLN.RVW).

True, as with David Brin's "The Transparent Society" (cf. BKTRASOC.RVW), Marlin-Bennett promises a unique premise, in this case a tie between privacy and intellectual property. Unlike Brin, in this book the link is not strongly demonstrated. We are, therefore, left with a somewhat simplistic review of the topics listed in the title.

copyright Robert M. Slade, 2006 BKKPIPIP.RVW 20061119
rslade@vcn.bc.ca slade@victoria.tc.ca

rslade@computercrime.org

<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

Search RISKS using [swish-e](#)

Volume 24: Issue 56

Sunday 4 February 2007

Contents

- [CastleCops 5-Year Anniversary](#)
[Rob Slade](#)
- [A second site "improves" security](#)
[FJ Reinke](#)
- [Re: There's more to worry about than math libraries](#)
[Richard Karpinski](#)
- [Re: Excel Date Bug](#)
[Steve Schafer](#) [R.G. Newbury](#) [Dik Winter](#)
- [Re: Daylight saving time mess looms](#)
[J R Stockton](#)
- [Re: Super Bowl site hacked](#)
[Rob Slade](#) [A.Lizard](#)
- [Re: The problem of abstractions ...](#)
[Jos Buurman](#) [David Cantrell](#) [Tony Finch](#) [Ben Hutchings](#) [Steve Schafer](#) [Ray Blaak](#)
[Christopher C. Stacy](#)
- [Re: Digital cameras converted to weapons](#)
[Steve Schafer](#)
- [Re: Canadian coins containing tiny transmitters](#)

[Rob Slade](#)

● [Re: Windows Vista voice vulnerability](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

✶ CastleCops 5-Year Anniversary

<Rob Slade <rMslade@shaw.ca>>

Sat, 03 Feb 2007 14:37:18 -0800

As one involved in malware research, I should note the fifth anniversary of CastleCops. (Actually, five years ago it was `computercops.biz`: it's only been CastleCops for a couple of years now.) CastleCops is a company, but promotes efforts involved in community and communication, primarily aimed at malware, spam, and phishing.

In regard to phishing, a recent project is Phishing Incident Reporting and Termination (PIRT, <http://wiki.castlecops.com/PIRT>). This project identifies phishing sites and gets them shut down, as well as providing information to law enforcement for prosecutions. It's been running less than a year, but has already saved an estimated (very conservatively) U\$22 million in prevented losses. (Anybody who wants to can submit phishing messages that you receive or URLs you identify to the project.)

To find out more about CastleCops you can visit `www.CastleCops.com`, or `de.CastleCops.com` if you Speak German, or `wiki.CastleCops.com` if you are into Wikis.

For their fifth anniversary, they are, naturally, having a contest:

http://www.castlecops.com/a6737-100_000_Contest_Celebration.html

(Brian Krebs (*The Washington Post*) blog:

http://blog.washingtonpost.com/securityfix/2007/01/in_praise_of_the_phish_fight_er.html)

rslade@vcn.bc.ca slade@victoria.tc.ca

rslade@computercrime.org

<http://victoria.tc.ca/techrev/rms.htm>

✦ A second site "improves" security

<"Reinke's Catch All Email" <reinkefj@yahoo.com>>

Wed, 24 Jan 2007 14:28:34 -0500

A second site, Paytrust, has followed Vanguard, in "improving" security. They now have one screen for userid and then a second screen for password. The theory is that if I don't see my selected picture and secret phrase on the screen then I shouldn't enter my password.

I think this is "security theater" at best?

While it makes phishers work a little harder. They have to be ready to execute a true man-in-the-middle attack. Not very difficult imho.

I don't understand how this helps ME. I understand that it gives them a more plausible defense should someone break in. Saying we tried.

It also asks me pre-established "extra" questions should I say

I'm using a public computer. Knowing the answers to questions that can be relatively easily found out, ain't gonna cut it. How this stops replay or a keystroke logger beats me?

This is all kabuki as opposed to real security. If they want a security model to follow, I like GoToMyPC's one time passwords.

That's protection.

Arghhh!

Ferdinand John Reinke, Kendall Park, NJ 08824
<http://www.reinke.cc/> blog: <http://www.reinkefaceslife.com/>

Re: There's more to worry about than math libraries (Robinson, R 24 54)

<Richard Karpinski <dick@cfcl.com>>

Fri, 19 Jan 2007 21:26:21 -0800

Boy, did you pick the wrong thing to complain about! The floating point arithmetic including on the X86 machines follows the IEEE 754 standard. Before 754 was developed, a programmer using floating point had to deal with many wild problems arising on every machine. Every new computer had a new floating point arithmetic which would bite you in unexpected ways.

Ordinary problems included cases where X times 1 was not equal to X, or Y plus 0 was not equal to Y. These particular cases involve having

insufficient extra precision, called guard digits, in the registers to accommodate fully accurate results, especially when the result required renormalization. In the bad old days you could thus not even count on add and multiply giving accurate results. Portable software, accurate to the bit, was well nigh impossible.

If you research the standard, you will find very well documented reference code for square root and even large collections of test cases suitable to guarantee that the results of allegedly conforming implementations really did meet those demands of the 754 standard. The current state of affairs is already far better than what you seem to be seeking. Without actually attending the working group meetings, you would have no idea how much care is embodied in that standard.

Richard Karpinski, World Class Nitpicker, 148 Sequoia Circle,
Santa Rosa,
CA 95401 dick@cfcl.com Home +1 707-546-6760 Cell +1 707-228-9716

✉ **Re: Excel Date Bug (Macintyre, [R 24 54](#))**

<Steve Schafer <steve@fenestra.com>>
Sat, 20 Jan 2007 21:46:40 -0500

Al Mac refers to a well-known Excel "bug" involving whether or not 1900 is considered to have been a leap year. What is apparently not so well known is the reason behind Excel's behavior: compatibility with Lotus 1-2-

3. I did some research on this a few years ago, and I wasn't able to trace the behavior further back than the first version of Lotus 1-2-3, so that seems to be when the actual bug was introduced.

You can read Microsoft's statement on it here:

<http://support.microsoft.com/kb/214326>

(Although that article refers specifically to Excel 2000, the issue was present long before that. I first learned of it in connection with Quattro Pro, which exhibits the same behavior for the same reasons, in 1992 or thereabouts.)

Steve Schafer, Fenestra Technologies Corp. <http://www.fenestra.com/>

✉ **Re: Excel Date Bug (Macintyre, [RISKS-24.55](#))**

<"R.G. Newbury" <newbury@mandamus.org>>
Sat, 03 Feb 2007 21:50:51 -0500

It gets better: Microsoft is attempting to fast-track its weird, wholly messed up, snafu'ed, tarfun'ed, version of an OOXML standard as ECMA 376, and that particular stupidity is BUILT RIGHT IN!...That is, rather than correct the error, any 'standardized' program must REPLICATE the error. Full story on groklaw, scroll down. Read the whole thing. BTW, the drop dead date for objections to the fasttrack process is February 5th. I

cannot find
anyone at the Standards Council of Canada who even knows that
the proposal
exists and that Microsoft will win approval for the fasttrack
process by
default if nothing is done.

⚡ Re: Excel Date Bug (Steve Wildstrom)

<Dik.Winter@cw.nl>

Sun, 4 Feb 2007 02:19:40 +0100 (MET)

It is hard for me to believe that nobody at Microsoft thought
about another
solution than they think about (maintaining the epoch and
increment the day
numbers for all days from 1 Mar 1900). The most obvious
solution would be
to decrement the day numbers before 1 Mar 1900, effectively
setting the
epoch one day later... The incompatibilities listed would only
occur when
dates before 1 Mar 1900 were used. And as is noted, that is
rare. And
the error noted is corrected. But perhaps this solution is too
rational?

dik t. winter, cw, kruislaan 413, 1098 sj amsterdam,
nederland, +31205924131
home: bovenover 215, 1025 jn amsterdam, nederland; [http://www.
cw.nl/~dik/](http://www.cw.nl/~dik/)

⚡ Re: Daylight saving time mess looms ([RISKS-24.55](#))

<Dr J R Stockton <reply0705@merlyn.demon.co.uk>>

Sun, 4 Feb 2007 17:46:38 +0000

That is inaccurate. The change is by four weeks in some years and five weeks in others. That shows the dangers of believing the media. Actually, DST is now always 34 weeks; it used to fluctuate.

The change of DST rules actually occurs on March 1st, according to the Act.

<URL:<http://www.merlyn.demon.co.uk/uksumtim.htm#AA>> refers.

John Stockton, Surrey, UK <http://www.merlyn.demon.co.uk/>

[Note spelling correction: Daylight saving (singular) time. PGN]

⚡ Re: Super Bowl site hacked (EEkid, [RISKS-24.55](#))

<Rob Slade <rMslade@shaw.ca>>

Sat, 03 Feb 2007 15:11:19 -0800

There were actually a number of these in operation. The Internet Security Operations Task Force (ISOTF) had quite a frenzy of activity on Friday, and most sites were taken down in short order. The sites attempted to use the VML vulnerability, so only those who had been unpatched for quite some time were at risk.

⚡ Re: Super Bowl site hacked, seeded with exploits ([RISKS-24.45](#))

<"A.Lizard" <alizard@ecis.com>>

Sat, 03 Feb 2007 16:02:16 -0800

I think the RISK here is running a Windows webserver/OS on a high-traffic website.

<http://www.reptilelabs.com> <http://www.ecis.com/~alizard> <http://www.pgpi.org>

Disaster prep info: <http://www.ecis.com/~alizard/y2k.html>

🔥 Re: The problem of abstractions ... (Robinson, [RISKS-24.54](#))

<"Jos Buurman" <the_jos@hotmail.com>>

Wed, 24 Jan 2007 18:32:03 +0100

I've read Paul Robinson's topic with great interest.

We (large institutional investor) use a system that's developed in APL by the supplier. The product is offered in the kitchen model, you can have the basic product which functions very well, you can also add numerous modules, the supplier knows how much time this takes on average.

The fact is that this is indeed a niche market. Furthermore, it's driven by external force. The financial markets determine the products the application should support. The market determines how those products are calculated.

For example, we had a minor valuation issue with some special government bonds and I could determine the cause by just setting the market's

calculation up in Excel. It turned out we forgot to set the right rounding rule. Those calculations are provided in detail by external parties, in this case the French Government.

If a supplier would invent it's own standards, this was not possible.

Also, it's a market where little mistakes do have large impact. The rounding error was on the 5th decimal, but on our holdings this could be several thousand Euros or more.

Since there is a large impact on error, companies are willing to pay. So that covers the financial aspects of development.

The financial market is also constant developing. New instruments seem to appear on daily basis. That also calls for modular set-up of the application.

Then this market for systems is small. There are not that many investment companies that can afford these kinds of systems. There are only a few suppliers. If a company screws up big time once or twice, it's out of business.

It's hard to compare this market to other markets. Most markets don't have customers with the financial power this market has. The market is driven by external forces (the financial markets) and not the developing companies. The financial products have clear specifications.

You can compare the market for railway systems or air traffic systems to ours. Those are markets with the same financial power, customer

driven,
clear specifications and high risk for the individual customer.

It's not that there are many huge errors out there. It's the same as the rounding 'error' we experienced. For many it's not significant. Only it could have an enormous impact in those systems.

Most of the time it's some kind of configuration mistake that leads to errors. Those happen in any system, even our modular APL based one.

Jos Buurman, System Administrator Investment Management

Re: The problem of abstractions ... (Robinson, [RISKS-24.54](#))

<David Cantrell <d.cantrell@outcometechnologies.com>>

Mon, 22 Jan 2007 10:21:48 +0000

Paul Robinson wrote:

> There is a guy named Louis Savain who ... wants to create for software
> what the transistor and the printed circuit did for electronics ...

Having rigidly defined interfaces between components doesn't help when you have large numbers of components. The interactions between groups of components can become *very* complex and can lead to bugs. We can draw an analogy with the game of Go. It has very simple rules governing the rigidly defined interfaces between board, players and pieces, but the interactions

between them lead to complexity such that precisely what will happen during a game is unpredictable.

This is of course a Good Thing as it means a mediocre player like me can still beat the computer at *something*.

> An example I gave was on the comparison between buying a kitchen makeover
> and a maintenance change to a software package.

A new kitchen is a fairly small, simple construction project. Small simple software projects are likewise frequently delivered on time, on budget, and working first time. You just don't hear about them because something that happens all the time ain't news. What you do hear about are the failed software projects of a complexity similar to that of the larger physical projects such as are par for the course in (for example) the defence industry.

> In short, we get away with the great kind of racket in our business that no
> one would tolerate from a Taiwanese manufacturer of toasters!

But we accept it from the manufacturers of our fighter aircraft, the builders of railways, and so on.

⚡ Re: The problem of abstractions ... (Robinson, [RISKS-24.54](#))

<Tony Finch <dot@dotat.at>>
Mon, 22 Jan 2007 13:27:02 +0000

I remember looking at Savain's web site <http://www.rebelscience.org/> a few months ago. He isn't completely wrong, but he does set off a lot of my kook alarms. Your summary of his ideas about programming is a fairly good description of Erlang, which has proven to reduce error and increase productivity and reliability, and it has been used on some large and successful commercial and open source projects. Savain's ideas boil down to diagrammatic programming and as far as I can tell he doesn't talk about abstractions larger than a statement or perhaps a procedure, i. e. he doesn't say how to build software in the large. On the other hand, Erlang does have a coherent answer to this problem - have a look at the thesis of Joe Armstrong, one of Erlang's creators.
http://www.sics.se/~joe/thesis/armstrong_thesis_2003.pdf

f.a.n.finch <dot@dotat.at> <http://dotat.at/>

✶ Re: The problem of abstractions ... (Robinson, [R 24 54](#))

<Ben Hutchings <ben@decadent.org.uk>>

Sat, 20 Jan 2007 22:17:34 +0000

- > If I understand his proposals, what he wants to do is develop software
- > visually in terms of components, and "wire" the components together.
- > Hardware has rigidly defined interactions and race conditions can't
- > occur because asynchronous operations are not possible.

Please take a look at some device drivers in an open source operating system. High-level hardware components such as PCI devices often have very complex interactions, massive internal parallelism, and timing characteristics that are hard to predict - and that's even if they don't have a processor and "firmware" of their own. It's generally far cheaper to work around hardware bugs in a device driver, if that's at all possible, than to re-spin the hardware. So I don't think computer hardware provides a particularly good example to us.

> An example I gave was on the comparison between buying a kitchen makeover
> and a maintenance change to a software package. With a kitchen, you can
> generally buy off-the-shelf components and have an almost exact estimate
> of the complexity, the time to finish and the cost. And everything will
> fit together and work right the first time.

Well, it makes a change from the tired old-car analogy.

Yes, you can buy these components off the shelf. They have fairly simple interactions with reasonably well standardised utility supplies. (Yet the sink does not abstract away the pipes below it; you have to remember not to put things down the plug hole that might build up in the pipe.) Your refrigerator isn't expected to interact with your hob. (Yet it does in an unfortunate way if you put them too close together.) When you cook a meal, all the burden of coordination is on you, not on the appliances and storage that are involved. This is not what people expect from

software: they expect a far higher degree of automation. A kitchen is not a good example either.

That's not to say that software can't be modular, with well-defined, tested, interfaces between modules. But I'm not sure that that's entirely possible or desirable for whole applications. Many of the requirements for an application will be a good deal "softer". And if the requirements change, that may require the interfaces between modules to change. If you wanted to do that in your kitchen, you'd be out of luck. But because you know software is more flexible, you expect to be able change the definitions of the components at any level - even if you don't know how long that will take!

> As it stands now, things are "good enough" to get by and even with all the
> failures we have, there is so much value for such little costs that we keep
> stumbling along.

In general, yes - though there are still seem to be many big projects with insufficient oversight from the customer that yield far less value than they cost - or even negative value. The software industry isn't going to stop doing this until its customers take charge and insist on ongoing refinement of requirements, phased delivery of and payment for working features, and other practices that help to reduce risk and increase value for money.
(They may even encourage greater modularity!)

⚡ Re: The problem of abstractions ... (Robinson, [R 24 54](#))

<Steve Schafer <steve@fenestra.com>>

Sat, 20 Jan 2007 21:46:40 -0500

Paul Robinson talks about "software integrated circuits" (pluggable software components with well-defined interfaces); we've heard it before. The reason it appears that we don't have such things today is that the proponents are comparing incomparable levels of abstraction. In fact, we do have them, in the form of if..then..else expressions, quicksort routines, TCP/IP stacks, etc. These are what correspond to off-the-shelf integrated circuits. And most software developers do use these components off the shelf.

What we don't have are things like pluggable accounting packages. It's true that software components of this sort, ones that could potentially be abstractable into generic packages, just aren't available. But hardware functionality of equivalent specific complexity isn't available, either. Instead, those who want to implement that kind of functionality in hardware turn to application-specific integrated circuits (ASICs), and ASIC development pretty much parallels software development:

- a) Implement.
- b) Test.
- c) Debug.
- d) Repeat from step (a).

There do exist modern programming languages that provide a much higher

level of abstraction than do mainstream languages like C/C++ and Java, without the extreme terseness of APL or the verbosity of Cobol. Haskell and other languages of the ML lineage come to mind. Ironically, one of the reasons they're not very popular is that they require the programmer to do more up-front thinking about the problem to be solved; i. e., they require more mental abstraction....

Steve Schafer, Fenestra Technologies Corp. <http://www.fenestra.com/>

✉ **Re: The problem of abstractions ... (Robinson, [RISKS-24.54](#))**

<Ray Blaak <rblaa@telus.net>>
Sun, 21 Jan 2007 21:55:28 -0800

Paul Robinson <paul@paul-robinson.us> writes:

> Basically he wants to create for software what the transistor and the printed circuit did for electronics ...

People keep coming up with this idea, and it keeps failing. Software components don't work this way. Things that are so rigidly defined so as to be perfectly reliable in unknown circumstances tend to be not very interesting or useful.

Visual programming tends not be expressive enough for the really useful types of things.

> Personally I believe he has some wonderful ideas and if he

isn't

> right he's very close. But right now, that's all he has, ideas.

That point is accurate. If he can make a system that proves he is right, then that would be a great success for everyone, really.

> Almost two years ago I wrote an article for comp.risks.[...] was wrong.

> Most of them not only didn't get the analogy, they didn't realize

> that most of their comments reinforced my points.

You only addressed one of the points. What about the others? In particular, I had said (in [RISKS-23.74](#)):

>> If you have small components that you know are right, and you then

>> combine those components to manipulate each other according to their

>> published interface specifications, the results should be consistently

>> correct. The results will be predictable, the usage will be consistent

>> every time.

> This is false. The results will not necessarily be correct at all.

> "Know are right" is not possible except in very specific and controlled

> contexts. When components are used in new situations, any existing

> assumptions cannot be relied on at all, without tedious and careful work

> to reestablish them.

> Software components are not physical components. They do not scale

> the same way.

>

> That the software industry does not offer the same reliability and

> quality as physically engineered products is not because

software

- > practitioners are pulling at fast one (although they often are, but for
- > different reasons).
- >
- > They don't offer the same guarantees, not because they don't want to, but
- > because they cannot. Getting software right is hard. Very hard. So
- > hard that even really really smart people are not willing to be on the
- > hook for it.
- >
- > Customers have to tolerate software with mistakes, because that is
- > the only way they can get affordable software at all. If they insisted
- > on the same guarantees, they wouldn't be able to pay for it.
- >
- > Yes, we need to make better software. We need to try. Things can be
- > improved. They must be. The current situation is not acceptable.
- >
- > But it is not easy. Humans don't seem to be good at it.

There is clearly a software problem that needs to be improved. How to do it is another question. Probably a mixed approach of little things will work over time (some formal methods, some better languages, etc.), but most of all it will require a greater attention to care and quality and a reduction of simple laziness.

- > The lessons of history teach us - if they teach us anything - that
- > nobody learns the lessons that history teaches us

True enough.

Ray Blaak rAYblaaK@STRIPCAPStelus.net

Re: The problem of abstractions ... (Robinson, [RISKS-24.54](#))

<"Christopher C.Stacy" <cstacy@dtpq.com>>

Mon, 22 Jan 2007 10:38:07 -0500

> ... The "big thing" in APL was to write a "one liner," an attempt to
> write a complete working application in one line of code.

Writing long complex expressions was not considered a positive aesthetic by experienced APL programmers when I was at STSC (the major APL timesharing service bureau) in the heyday of the late 70s. We preferred (and taught clients) to write good styled code, particularly avoiding long lines, and of course to put comments on them. Of course, one can write poor style code in APL, as in any language, and perhaps you saw some.

I would take issue with the characterization that APL "failed dismally", although unfortunately it is not very popular today outside of the actuarial and other niche markets. APL was quite popular for while, and represented a major success story for many organizations. I don't understand your statement that during that time it "became difficult to work with", or that its abstraction capabilities had anything to do with it's lack of popularity.

It is possible to write bad, incomprehensible, unmaintainable code in any programming language. The difference with APL is that you have

a language
in which it is possible to express certain things concisely and
more
clearly. (Other languages let you express certain other things
very well,
too. And some other languages seem most conducive to certain
loud vocal
expressions.)

I don't understand your comment about "subroutine libraries" at
all; it
seems to be a nonsequitur. The APL language consists of a large
number of
primitive operators that correspond to what would have to be
subroutines in
other languages. APL vendors provided systems which
additionally included
hundreds of library packages for database, graphics, and many
kinds of
sophisticated application libraries.

> Some people have said similar things about Lisp and the
increase in
> productivity they have seen from that as well.

Well, people say all kinds of things, but that doesn't mean that
they know
what they are talking about.

I have used, and continue to use, a lot of programming languages
since I
started programming in 1973. I haven't used APL since the
1970s; I switched
to Lisp for most of my work around 1981, and Lisp is I'm using
right now for
most of my projects. I would heartily agree that Lisp and APL
are powerful
tools that allow good programmers to maximize their productivity.

Everyone agrees that appropriate abstractions are essential for
good
programs, and that some languages are better at facilitating
that.

Unfortunately, most discussion of particular languages consist of repetition of myths and misunderstandings and misinformation, with religious overtones and attendant rationalizations.

There are many Risks involved in analyzing the various aspects of programming languages and their effectiveness. One of the most common failures is trying to correlate popularity of a language with vague assertions or just plain wrong information about its technicalities.

I hope that Risks Digest doesn't engage in such endless religious "language wars". It would however be instructive to illustrate both general and language-specific flaws, traps, and risks by analyzing systems failures that have actually occurred.

✶ **Re: Digital cameras converted to weapons (Markowitz, [R 24 54](#))**

<Steve Schafer <steve@fenestra.com>>

Sat, 20 Jan 2007 21:46:40 -0500

Sidney Markowitz writes, "The article on converting a camera to a 'taser' incorrectly talked about disposable digital cameras, which do not currently exist."

I happened to see one on the shelf at a CVS Pharmacy today:

[http://www.cvs.com/CVSApp/cvs/gateway/detail?prodid=274180
&previousURI=/CVSApp/cvs/gateway/search?ActiveCat=499
^Query=camera+digital](http://www.cvs.com/CVSApp/cvs/gateway/detail?prodid=274180&previousURI=/CVSApp/cvs/gateway/search?ActiveCat=499^Query=camera+digital)

(URL manually broken across lines.)

Steve Schafer, Fenestra Technologies Corp. <http://www.fenestra.com/>

✶ Re: Canadian coins containing tiny transmitters ([RISKS-24.54](#))

<Rob Slade <rMslade@shaw.ca>>

Sat, 03 Feb 2007 15:11:19 -0800

Well and thoroughly debunked. The initial report was from a US intelligence analysis group, with no details. When tasked on the matter, they first asserted it was true, and finally admitted that there was no evidence at all to support the claim. The idea of bugging coins was widely seen as a stupid idea, since most such devices would have ended up in vending machines ...

[Noted by many of you. PGN]

✶ Re: Windows Vista voice vulnerability ([RISKS-24.55](#))

<Rob Slade <rMslade@shaw.ca>>

Sat, 03 Feb 2007 15:11:19 -0800

And it would be easy enough to have the voice/video file mail itself out to email addresses harvested on the machine, turning it viral ...



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 57

Weds 21 February 2007

Contents

- [Govt Health IT: Electronic prescribing is no panacea](#)
[Deborah Peel](#)
- [DNS roots attacked](#)
[PGN](#)
- [AACCS: A Tale of Three Keys, by J. Alex Halderman](#)
[via Monty Solomon](#)
- [Amazing boilerplate text in Fairfax County e-mail](#)
[Gabe Goldberg](#)
- [Crashing an in-flight entertainment system](#)
[Steve Summit](#)
- [Infrastructure risks: pump-station alarm](#)
[Matt](#)
- [Carmakers copy and repeat error almost forever](#)
[Doug McIlroy](#)
- [Two war stories from the NASA trenches](#)
[Ron Garret](#)
- [US government's contracts tracked by contractors](#)
[Ken Knowlton](#)

- [Study Finds Security Flaws on Web Sites of Major Banks](#)
[Gabe Goldberg](#)
 - [Web Site Wants JPEG of Government ID](#)
[Mike Conley](#)
 - [Re: Math libraries](#)
[Peter B. Ladkin](#)
 - [Re: Excel Date Bug](#)
[John Levine](#)
 - [Impact of DST changes on BlackBerry device users](#)
[Monty Solomon](#)
 - [Re: Digital cameras converted to weapons](#)
[Leonard Finegold](#)
 - [Re: Canadian coins containing tiny transmitters](#)
[Adam Abrams](#)
 - [New Short Video: "Is Your Cell Phone Bugged?"](#)
[Lauren Weinstein](#)
 - [REVIEW: "Code Quality: The Open Source Perspective", Diomidis Spinellis](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

Govt Health IT: Electronic prescribing is no panacea

<"Dr. Deborah Peel" <dpeelmd@patientprivacyrights.org>>

Sun, 18 Feb 2007 00:27:48 -0600

You should know about this massive violation of the privacy of every American who takes medication.

This opinion piece is about the fact that there is no such thing as a private prescription in the nation. Identifiable prescription data is sold to insurers for medical underwriting and to large employers to use as they see fit (discrimination?).

Electronic prescribing is no panacea

By Dr. Deborah Peel, Saturday, February 17, 2007

<http://www.governmenthealthit.com/article97686-02-19-07-Print>

When a coalition of technology companies, insurers and health care providers launched a \$100 million project last month to provide free electronic prescribing software to every physician in the United States, it was greeted with cheers. The presence of brand name vendors was supposed to ensure that sensitive prescription records would be private and secure.

But those who believe there is anything private about e-prescribing under the National ePrescribing Patient Safety Initiative (NEPSI) - or any other e-prescription system - are simply incorrect.

Security makes little difference because every identifiable prescription in the country is data mined and sold daily. Nobody needs to break into pharmacies to steal our prescriptions; they are for sale. For example, market intelligence firm IMS Health reported revenues of \$1.75 billion in 2005 solely from the sale of prescription records, primarily to drug companies.

Privacy is the right to control who sees your sensitive health records and the right to decide if those records are even entered into electronic systems. But it is impossible for anyone to have a private prescription - meaning that it is never disclosed without a patient's consent - because data mining has eliminated that right.

Furthermore, many people refuse to take psychiatric medication or other medications in an attempt to prevent the pharmacy benefits management industry from reporting to employers that they are on antidepressants or other medications.

Knowing that prescriptions are not private also keeps people with other sensitive illnesses from taking medications. And that exerts pressure on doctors to avoid prescribing pain medications - out of concern that the Drug Enforcement Administration is tracking their prescribing patterns. The lack of prescription privacy is a problem that endangers people's lives and quality of life.

That brings us to more misinformation about e-prescribing: that it is a panacea for preventing prescription errors. Pharmacies have been converting handwritten prescriptions into electronic prescriptions for more than a decade, so software that catches errors and drug interactions could have been used before with electronic prescription data. Doctors don't need to issue e-prescriptions to reap the benefits of software that checks for correct doses and a drug's conflicts with other medications.

In the rush to extol the benefits of e-prescribing, NEPSI also neglects to mention that e-prescribing will introduce new sources of error. It could produce about the same rate of errors as written prescriptions.

With written prescriptions, two licensed professionals - the physician

and the pharmacist - look at the prescription. Two experienced humans are paying attention. If there are any questions, the pharmacist calls the doctor. With e-prescribing, only one human will look at the e-prescription, the doctor. Indeed, e-prescribing may make errors more common than when doctors write prescriptions.

Most people do not know that they cannot keep prescription records private - it's a huge area of ignorance. Now that we are moving rapidly into an e-health system, we need to build it right. Congress should follow the lead of New Hampshire, which passed a law in 2006 to stop illegal and unethical prescription data mining.

We need all the benefits that health information technology can bring, but we also need privacy. Technology can provide both - we should never have to choose between our privacy and our health.

Peel is a physician and chairwoman of the Patient Privacy Rights Foundation based in Austin, Texas.

DNS roots attacked

<"Peter G. Neumann" <neumann@csl.sri.com>>
Tue, 6 Feb 2007 17:19:19 PST

Hackers briefly overwhelmed at least three of the 13 computers that help manage global computer traffic Tuesday in one of the most significant attacks against the Internet since 2002. Experts said the unusually

powerful attacks lasted for hours but passed largely unnoticed by most computer users, a testament to the resiliency of the Internet. Much rogue data was traced to South Korea. UltraDNS was a particular target. Attacks passed largely unnoticed by most computer users. [Source: AP item, 6 Feb 2007, PGN-ed; Thanks to Lauren Weinstein.]

<http://www.cnn.com/2007/TECH/internet/02/06/internet.attacks.ap/index.html>

[See [RISKS-22.32](#) for the attacks that crippled 9 of the 13 root servers in Oct 2002. Perhaps the Internet is somewhat more robust now? PGN]

⚡ AACS: A Tale of Three Keys, by J. Alex Halderman (Re: [RISKS-24.55](#))

<Monty Solomon <monty@roscom.com>>
Sat, 17 Feb 2007 11:35:21 -0500

This week brings further developments in the gradual meltdown of AACS (the encryption scheme used for HD-DVD and Blu-Ray discs). Last Sunday, a member of the Doom9 forum, writing under the pseudonym Arnezami, managed to extract a "processing key" from an HD-DVD player application. Arnezami says that this processing key can be used to decrypt all existing HD-DVD and Blu-Ray discs. Though currently this attack is more powerful than previous breaks, which focused on a different kind of key, its usefulness will probably diminish as AACS implementers adapt.

To explain what's at stake, we need to describe a few more details about the way AACS manages keys. Recall that AACS player applications and devices are assigned secret device keys. Devices can use these keys to calculate a much larger set of keys called processing keys. Each AACS movie is encrypted with a unique title key, and several copies of the title key, encrypted with different processing keys, are stored on the disc. To play a disc, a device figures out which of the encrypted title keys it has the ability to decrypt. Then it uses its device keys to compute the necessary processing key, uses the processing key to decrypt the title key, and uses the title key to extract the content. ...

<http://www.freedom-to-tinker.com/?p=1121>

✶ Amazing boilerplate text in Fairfax County e-mail received today

<Gabe Goldberg <gabe@gabegold.com>>

Mon, 05 Feb 2007 17:20:04 -0500

The following hard-to-believe text speaks for itself. Fairfax County (VA) prides itself on being techno-savvy, on the cutting edge of the new economy, and other similar blather. Looks like the "cutting edge" is severing Fairfax from the Internet. Being offline would be bad enough, but bouncing e-mail? For three or four days? Amazing. I wonder how many people won't know in

advance and will be baffled/frustrated/angered/outraged?

*** Fairfax County information technology services will be unavailable

beginning February 17 and resume on February 20. My account will be

inaccessible during this timeframe and any incoming e-mail will be bounced

to the sender. In effect, Fairfax County will temporarily cease to exist

online for this period. We apologize for the inconvenience.***

✈️ Crashing an in-flight entertainment system

<Steve Summit <scs@eskimo.com>>

Wed, 21 Feb 2007 00:16:08 -0500

Hugh Thompson reports that he was able to get an airplane's in-flight entertainment system into a significantly unexpected state, by (a) using a numeric keypad, rather than the normal up/down buttons, to enter a value one higher than a Tetris game's preference was intended to allow, then (b) using the normal "up" button to increment the value still further -- evidently the programmer had implemented "if(value == 4) {don't increment}" rather than the more robust "if(value >= 4)". When he incremented the value past 127, not only his screen, but every seat-back screen on the whole plane went black, until a flight attendant reset the system. Further details at <http://blogs.csoonline.com/node/151> [with some subsequent discussion].

⚡ Infrastructure risks: pump-station alarm

<"Matt">

Tuesday, 5 Feb 2007 13:55:00 -0500 (EST)

A tree-trimming contractor clearing power lines cut a phone line which serviced a pump-station alarm. The alarm is supposed to be checked twice daily, but the pump was out of commission for four days, leading to a massive sewage spill.

http://www.charlotte.com/mld/charlotte/news/16593620.htm?source=rss&channel=charlotte_news

The risks are clear; multiple single points of failure (the alarm, the phone line, the pump station, the human verification), no method to check for a failure of the alarm, and a possible flaw in the human logging / reporting side of things.

⚡ Carmakers copy and repeat error almost forever

<Doug McIlroy <doug@cs.dartmouth.edu>>

Sun, 18 Feb 2007 14:25:50 -0500

[RISKS-16.3](#), 5 May 1994, contained an account of the shock of being locked out automatically after closing the door on a stopped car with the engine running. (Not unlikely if you get out to check the roof rack,

fetch the
mail, etc.) The problem was reported for a Chevy; I met it
years later in
a 2001 Ford Focus. Poking around the web, I find reports of the
same
trouble in car models as recent as 2006 from various makers.
Disheartening
that such a trivially fixable misfeature should be imitated so
widely and
persist so long.

⚡ Two war stories from the NASA trenches

<Ron Garret>

Wed, 7 Feb 2007 23:55:32 -0800

One of my favorite case studies is getting a bit long in the
tooth, but it
has never to my knowledge been cited or discussed in RISKS, so
from the
better-late-than-never department I give you:

<http://ase.arc.nasa.gov/publications/pdf/2000-0176.pdf>

This is the story of the NASA Deep Space 1 Remote Agent
Experiment (RAX),
and a bug that appeared in the RAX executive despite a then-
state-of-the-art effort to develop fault-free software. The
approach was
very much like the "software-IC" approach that has been
advocated off and on
for decades (I remember first hearing about it when I was a grad
student,
and a 5MB hard drive was considered a lot of storage). To
summarize and
radically oversimplify, a "substrate" layer was developed and
exhaustively
analyzed using formal methods to insure that it maintained

certain
invariants (like being deadlock- free). Application code was
then developed
on top of this exhaustively analyzed substrate, in effect
"wiring together"
the supposedly reliable components.

To make a very long story much too short, one of the applications
programmers inadvertently undermined the invariants that were
supposed to be
guaranteed by the substrate when he needed a feature that the
substrate
didn't provide. Instead of requesting that the feature be added
to the
substrate, he just "rolled his own" (it was only two lines of
code), and
thereby undermined the guarantees that the substrate provided.
The
resulting bug was never detected during extensive ground
testing, but
nonetheless failed in flight.

It was quite a humbling experience, and it makes a worthwhile
read even
today.

As long as I'm telling war stories, I'll offer up a second one
which was
never published. This happened in 1989.

We were developing code for autonomous mobile robots (what was
to eventually
become the Mars Pathfinder mission) using a dialect of Lisp
called T. We
had ported the T compiler from a Sun3 to a Heurikon 680x0 board
running
vxWorks. We found that when the robot moved its arm the Lisp
process would
crash intermittently. Forensic analysis after the crash
revealed a
completely and nondeterministically corrupted heap.

This was the probably the most challenging bug I've ever

encountered in my career because it was impossible to reliably reproduce, and when it happened it obliterated everything that might provide a clue as to why it happened. Another long story short (it took us over a year to figure it out) the problem turned out to be a bug in the T compiler: in the code emitted to return from a function, the stack pointer was adjusted while they were still live vales on the stack. On the Sun this was not a problem because user processes ran in a different address space from the kernel. But under vxWorks interrupt handlers used the same stack as the process being interrupted. So when an interrupt happened right in between those two instructions the unprotected value on the stack was obliterated by the interrupt handler code, resulting in a gradual corruption of the heap.

The moral of the story is that even code that tests perfectly under formal analysis and/or extensive use may yet contain latent bugs.

🚀 US government's contracts tracked by contractors

<Ken Knowlton <KCKnowlton@aol.com>>

Mon, 5 Feb 2007 18:09:32 EST

(From AOL's NY Times news section, pertinent to "RISKS" for several reasons.

Complete article: <http://www.nytimes.com/2007/02/04/washington/04contract.html>

Contractors still build ships and satellites, but they also collect income taxes and work up agency budgets, fly pilotless spy aircraft and take the minutes at policy meetings on the war. They sit next to federal employees at nearly every agency; far more people work under contracts than are directly employed by the government. Even the government's online database for tracking contracts, the Federal Procurement Data System, has been outsourced (and is famously difficult to use).

Study Finds Security Flaws on Web Sites of Major Banks

<Gabe Goldberg <gabe@gabegold.com>>

Mon, 05 Feb 2007 09:02:02 -0500

Internet security experts have long known that simple passwords do not fully defend online bank accounts from determined fraud artists. Now a study suggests that a popular secondary security measure provides little additional protection. [Source: Brad Stone, *The New York Times*, 5 Feb 2007]

<http://www.nytimes.com/2007/02/05/technology/05secure.html?th&emc=th>

http://topics.nytimes.com/top/reference/timestopics/people/s/brad_stone/index.html?inline=nyt-per

Web Site Wants JPEG of Government ID

<Mike Conley <nomad@mac.com>>

Sun, 18 Feb 2007 12:17:45 +0000

I recently visited a Web site, <<http://www.istockphoto.com>>, which provides low-cost downloads of photographic images submitted by registered users. It's actually quite nice, and rather professional-looking, and I was interested in uploading some of my photos and perhaps making a few dollars on them.

I discovered while registering that, in order to upload images, one has to establish an upload account, a requirement for which is the submission, over the Internet, of a scanned JPEG image of a government-issued identity document, such as a driver's licence or -- even better -- a passport.

Further comment doesn't really seem necessary.

✶ Re: Math libraries (Robinson, [R 24 54](#), Karpinski, [R 24 56](#))

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>

Mon, 05 Feb 2007 09:03:49 +0100

Dick Karpinski suggests in [RISKS-24.46](#) that Paul Robinson's worries about the hardware math functions in the 586 class of processors are not as well founded as his worries about software math functions. I concur. Dick could have told more of the history.

William Kahan at U.C. Berkeley has been worrying about floating

point

calculations in computers for the last four decades and won the Turing

Award, the highest award for technical contributions to computing science,

in 1989 for these efforts. Intel was interested in defining portable

accurate floating point computations, in advance of their introduction of

the math coprocessor for the i8086/8 series (i.e., what was to become the

8087). Impressed by Kahan's understanding of the problems as well as his

efforts on behalf of Hewlett Packard, Intel engaged him to help further this

cause. Kahan worked with a PhD student of his, Jerry Coonen, and Harold

Stone, to define a proposal for the IEEE p754 committee which became in

large part the IEEE 754 standard. One can read more about it in some notes,

for an IEEE Computing article in 1998, on Kahan's WWW site at <http://www.cs.berkeley.edu/~wkahan/ieee754status/754story.html>

I was the Teaching Assistant for the graduate numerics course in the Math

Department at UCB at the time that Jerry took it. Assessing the assignments

was a breeze. One first looked at Jerry's solutions and those of Jamie

Sethian (now himself a math professor at U.C. Berkeley) to see how to do it

right. (Those are the advantages of graduate teaching-assisting at a place

such as U.C. Berkeley. You can always assume that there is at least one

student who is better than yourself, and sometimes more.) Jerry finished his

PhD, on the FP work, waaay before I finished mine. I remember him telling me

that the way to be certain of a good job was to become acquainted with every

line of the BSD source code. Those were the days. But even in

those days it was expanding faster than one could read it (besides, that was not the right way to get a PhD in Logic and the Methodology of Science, for probably more than one reason :-).

To my mind, IEEE 754 is one of the success stories in our efforts to reduce mistakes in computing. It is a pity certain spreadsheet programmers didn't emulate its example.

Peter B. Ladkin, Causalis Limited and University of Bielefeld
www.causalis.com www.rvs.uni-bielefeld.de

⚡ Re: Excel Date Bug (Winter, [RISKS-24.56](#))

<John Levine <johnl@iecc.com>>
5 Feb 2007 01:16:58 -0000

> The most obvious solution would be to decrement the day numbers before 1
> Mar 1900, effectively setting the epoch one day later...

That's what Open Office does. Dates in 1-2-3 and most spreadsheets are internally represented as integers with 1-Jan-1900 as day 1. In Open Office, day 1 is 31-Dec-1899, so dates before 1-Mar-1900 are off by one day.

This does not necessarily improve the situation. In spreadsheets I've seen, it's quite common to enter dates simply as dates, to mark when something happened, less common to do date arithmetic, and I've never seen anyone

doing date arithmetic as far back as 1900. So this change fixes the date arithmetic, at the cost of making dates before March 1900 display wrong.

I am not a big fan of Microsoft, but in this case I have to agree with them that there's no change to this bug that will make the situation better than it is now. They clearly did think about this change, and rejected it for sensible reasons.

John Levine, johnl@iecc.com, <http://www.johnlevine.com>

✶ Impact of DST changes on BlackBerry device users

<Monty Solomon <monty@roscom.com>>

Mon, 19 Feb 2007 20:05:57 -0500

Impact of North American Daylight Saving Time changes in 2007 on BlackBerry device users:

<http://www.blackberry.com/select/dst2007/>

✶ Re: Digital cameras converted to weapons ([R 24 54,56](#))

<Leonard Finegold <L@drexel.edu>>

Sun, 4 Feb 2007 18:43:21 -0500

Everyone is right:

At \$13.99 this "Digital" camera looks suspiciously like CVC's ye olde

chemical-type cameras of about the same price. I strongly suspect that what CVC calls "Digital" on the box (note they say "Simple Digital Processing") is what we mortals would call non-digital.

'The question is,' said Alice, 'whether you can make words mean so many different things.' Alice in Wonderland, CL Dodgson

Leonard X. Finegold, Physics, Drexel University, Philadelphia PA 19104 USA
L@drexel.edu Phone 215.895.2740

✶ Re: Canadian coins containing tiny transmitters

<Adam Abrams <adamabrams@shaw.ca>>
Sun, 04 Feb 2007 21:32:24 -0800

There was a followup story in which the Defense Department reversed themselves. There were no transmitters.
<http://edition.cnn.com/2007/TECH/01/19/canada.spy.coins.ap/>

I think some American contractors just thought the Canadian coins (probably the thick two-dollar coin which has a gold inner part and a silver outer part) looked funny and a wild idea became a rumour, which became a "reported fact".

With field intelligence like that, the "war on terror" will be won any day now, I'm sure...

Adam Abrams adamabrams@shaw.ca (604) 685-7634 www.adamabrams.com

🔥 New Short Video: "Is Your Cell Phone Bugged?"

<Lauren Weinstein <lauren@vortex.com>>

Fri, 16 Feb 2007 21:13:01 -0800

Greetings. I've been getting lots of continuing interest and queries in the wake of my blog item from late last year: "How To Tell If Your Cell Phone Is Bugged" (<http://lauren.vortex.com/archive/000202.html>).

In an effort to explain this issue in a more demonstrative and somewhat less technical manner, I'm pleased to announce a short free video (under six minutes): "Is Your Cell Phone Bugged?"

While I'll admit that the production values are much closer to those of Ed Wood than of Cecil B. DeMille, I hope you'll still find this video to be interesting, or at least amusing.

"Is Your Cell Phone Bugged?" Video Access Pages:

YouTube (Streaming):

<http://www.vortex.com/cellbug-vid-youtube>

Google Video (Streaming & Download):

<http://www.vortex.com/cellbug-vid-google>

Lauren Weinstein +1-818-225-2800 <http://www.pfir.org> <http://www.vortex.com>

<http://daythink.vortex.com> lauren@vortex.com or lauren@pfir.org

REVIEW: "Code Quality: The Open Source Perspective", Spinellis

<Rob Slade <rMslade@shaw.ca>>

Tue, 20 Feb 2007 10:40:40 -0800

BKCQTOSP.RVW 20061229

"Code Quality: The Open Source Perspective", Diomidis Spinellis, 2006,

0-321-16607-8, U\$54.99/C\$73.99

%A Diomidis Spinellis www.spinellis.gr/codequality dds@aueb.gr

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

M3C 2T8

%D 2006

%G 0-321-16607-8

%I Addison-Wesley Publishing Co.

%O U\$54.99/C\$73.99 416-447-5101 800-822-6339 bkexpress@aw.com

%O <http://www.amazon.com/exec/obidos/ASIN/0321166078/>

[robsladesinterne](#)

<http://www.amazon.co.uk/exec/obidos/ASIN/0321166078/>

[robsladesinte-21](#)

%O <http://www.amazon.ca/exec/obidos/ASIN/0321166078/>

[robsladesin03-20](#)

%O Audience a+ Tech 3 Writing 2 (see [revfaq.htm](#) for explanation)

%P 569 p.

%T "Code Quality: The Open Source Perspective"

The preface points out that it is easy to test for the functional requirements of an application: either the program performs the function or

it doesn't. Nonfunctional requirements (including such characteristics as

reliability, portability, usability, interoperability, adaptability,

dependability, and maintainability) are much harder to assess, and yet may

be more important. (In an automated train system, for example, the lack of

a function to change the schedule from within a given train still allows you

to use the train within a given schedule. Unreliability of the braking system means the system is worse than useless.) In addition, "Code Reading" (the title of Spinellis' previous book) is pointed out as the most common activity for developers, and yet is a skill seldom taught in the programming curriculum. The author has avoided using fictional code for the examples in this (and the prior) work by providing sample code from open source software projects, thus using working (but available) source code for illustrations.

Chapter one introduces the structure of the text by mapping characteristics from the ISO 9126 quality standard to the chapters and sections of the book. Inherent conflicts between different aspects of quality are also noted.

(For example, large numbers of discrete operations enhance the functionality of a system, but at some cost in terms of usability.)

Reliability is examined, in chapter two, in terms of common flaws. Examples of such flaws are given, followed by an explanation of the specifics of the problem. This is followed by samples of code that address the problem stated. Each point and section is accompanied by questions and discussion points that could be used in a course teaching the issues of code quality. (Unlike all too many sets of questions these are rigorous and challenging. Sometimes they may be a little bit too demanding: occasionally the discussion would require intimate knowledge of the internals of a specific programming language.) The chapter ends with a summary of the points and factors covered.

Various security vulnerabilities and coding points are illustrated in chapter three, but, in comparison to the rest of the work, this material is weak and disappointing. Performance issues in relation to time are reviewed in chapter four, and to space in five. The different factors of latency and bandwidth, and the trade-offs between memory and speed are noted. It is rather odd that Spinellis is at pains to point out that time efficiencies negatively affect simplicity and portability, while he goes to great lengths to provide suggestions for space optimizations for a variety of specific architectures (which wouldn't help portability either).

Chapter six looks at a number of factors relating to portability, between both hardware and operating system platforms. Maintainability is the longest chapter (seven) in the book, and bears the closest relation to Spinellis' previous work on "Code Reading." There is a special section on the characteristics of object-oriented code. Chapter eight, on floating point arithmetic, notes the sometimes surprising sources of inaccuracy.

In the information technology and development fields we are constantly obsessed with production of code and the speedy release of the next version. We need to stop and take a good look at the quality of what we produce: as it frequently stated, the greatest source of computer problems is computer solutions. In regard to security, it is demonstrably true that the exploits and difficulties that we find are those that would never have

been created
if only programmers had paid a little more attention to the
fundamental
concepts they were first taught. I believe Spinellis' text
should be
required reading for all programming courses and programs. In
addition,
those involved with analysis, maintenance, and change control
should
consider it a bible to be read and re-read until the lessons are
firmly
implanted.

copyright Robert M. Slade, 2007 BKCQTOSP.RVW 20061229
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<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

Search RISKS using [swish-e](#)

Volume 24: Issue 58

Thursday 1 March 2007

Contents

- [USAF F-22A jets grounded by software glitch](#)
[PGN Jeremy Epstein](#)
- [Briz-M rocket booster explodes over Australia](#)
[Mark Luntzel via PGN](#)
- [Software error reportedly contributed to sudden Dow-Jones drop](#)
[PGN](#)
- [Don't compute and drive at the same time...](#)
[Paul Saffo via PGN](#)
- [Risk of not knowing technology: jail](#)
[Ronald J Bottomly](#)
- [The Risks of Updating 80 Year Old Equipment](#)
[Chuck Weinstock](#) [Jim Geissman](#)
- [RFID tracking](#)
[Paul Wallich](#)
- [Putting the SSN genie back in the bottle?](#)
[Steve Summit](#)
- [Re: DNS roots attacked](#)
[Robert Graves](#) [R A Lichtensteiger](#) [Joe St Sauver](#)

- [Re: Crashing an in-flight entertainment system](#)
[PGN](#)
 - [Re: Amazing boilerplate in Fairfax County e-mail](#)
[Mark Brader](#)
 - [Disposable digital Cameras are truly digital](#)
[Jason Mechler](#)
 - [Carmakers copy and repeat error almost forever](#)
[Mark Brader](#)
 - [WOTE 2007 CfP](#)
[Josh Benaloh](#)
 - [REVIEW: "The Art of Software Security Assessment", Dowd et al.](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈ **USAF F-22A jets grounded by software glitch**

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

Mon, 26 Feb 2007 14:32:19 PST

The F-22 continues to encounter bumps in its first air expeditionary force deployment to Okinawa. The 12 aircraft from Langley AFB, Va., spent an unscheduled week at Hickam AFB, Hawaii, after the leading four had to abort the trip's last leg. As the Raptors reached the International Date Line, the navigation computers locked up, so the aircraft returned to Hickam until a software patch was readied. "Apparently we had built an aircraft for the Western Hemisphere only," says a senior U.S. Air Force official. When the F-22s arrived at Kadena AB, Okinawa, some Japanese citizens held a protest against the aircraft's noise. [Source: Aviation

Week & Space Technology, 26 Feb 2007, p.18; thanks to John Rushby and

Martyn Thomas for that item. PGN]

Gene Spafford noted another article:

<http://www.dailytech.com/Lockheeds+F22+Raptor+Gets+Zapped+by+International+Date+Line/article6225.htm>

✶ USAF F-22A jets grounded by software glitch

<Jeremy Epstein <jepstein@webmethods.com>>

Fri, 23 Feb 2007 15:55:52 -0500

Navigational systems failed, planes forced to return to Hawaii [visually having to follow their tankers to safety]. The problem turns out to be software (no surprise there). Fix created, "verified", installed, and they're off again.

"A spokesman for Lockheed Martin this week insisted that the navigation software problem was minor. 'The issue was quickly identified in a matter of days and a fix installed in the airplanes, which were flown successfully to Japan,' he said. 'There are 87 of these exceptional fighters and they are out there performing exceptionally well, and their pilots continue to fly them in new and greater ways.'"

Gee, I feel better knowing that.

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9011691&source=NLT_PM&nid=8

[Long ago there was an urban legend about the F-16 flipping over and flying upside down when it crossed over the equator. That report emerged because a consequential software flaw had actually been DETECTED in simulation, and had been FIXED before it could have happened in actual flights. However, the F-22 Raptor was presumably unwrapped without the benefit of rapter simulation, testing, and other pre-flight analyses. This smacks of Alpha males doing Beta testing by risking their own Gamma globulin. PGN]

🚀 Briz-M rocket booster explodes over Australia

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

Thu, 22 Feb 2007 10:02:37 PST

> Date: February 21, 2007 9:32:24 AM PST
> From: SpaceWeather.com <swlist@spaceweather.com>
> Subject: Major Breakup Event over Australia
>
> Space Weather News for Feb. 21, 2007, <http://spaceweather.com>
>
> On February 19th, late-night sky watchers across Australia witnessed a
> bright explosion followed by a debris cloud that hung in the sky for
> nearly an hour. At first a mystery, the source of the blast is now
> understood. It was a Russian Briz-M rocket booster misplaced in orbit
> last year by the failed launch of an Arabsat communications satellite.
> The fuel tanks of the Briz-M ruptured on Feb. 19th, producing

a vivid
> naked-eye display and more than 1000 pieces of debris.
Experts are
> calling this a "major breakup event," comparable to or even
worse than
> last month's Chinese anti-sat test. Visit <http://spaceweather.com> for
> more information and pictures of the Briz-M breakup.

[Thanks for spotting this one to Mark Luntzel, who particularly noted the ambiguous concept of "misplaced in orbit". PGN]

Software error reportedly contributed to sudden Dow-Jones drop

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

Wed, 28 Feb 2007 11:37:15 PST

On 27 Feb 2007, the Chinese stock market experienced a 9% drop. This apparently inspired heavy selling on the New York Stock Exchange, with a volume about twice normal. At one time, the calculation of the Dow Jones Industrial average was running about 70 minutes behind. Recognizing some sort of computer problem, DJ switched to a backup computer, which over a period of about three minutes caught up -- resulting in the posted average dropping about 240 points in those three minutes. This evidently led to some further panic selling. (At one point, the market was down 546 points, although it later recovered to close down only 416.) The cause of the software problem is under investigation. [Sources: Swiftnews of Dow Drop

Due to Computers (The Associated Press), *The New York Times*,
27 Feb 2007;

A Glitch in the Financial Matrix: How Heavy Trade Volumes and a
70-Minute

Time Lag Wreaked Havoc Upon the New York Stock Exchange, Dan
Arnall, ABC

News, 27 Feb 2007; starkly PGN-ed]

⚡ Don't compute and drive at the same time...

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

Tue, 27 Feb 2007 12:02:23 PST

[Many thanks to Paul Saffo for finding this item. (He
observed that this
gives a new meaning to the concept of a "Windows crash"...
PGN]

A man who authorities say appeared to be driving while using his
laptop
computer died Monday when his vehicle crossed into oncoming
traffic and
collided with a Hummer. After the crash, California Highway
Patrol officers
found the victim's computer still running and plugged into the
cigarette
lighter of his 1991 Honda Accord. ... [Source: Man in fatal
crash thought
to be using laptop, Associated Press, 26 Feb 2007]
[http://www.latimes.com/news/local/la-me-laptop27feb27,0,6942169.
story?coll=la-default-underdog](http://www.latimes.com/news/local/la-me-laptop27feb27,0,6942169.story?coll=la-default-underdog)

⚡ Risk of not knowing technology: jail

<"Ronald J Bottomly" <bottomly@erols.com>>

Thu, 22 Feb 2007 16:50:36 -0500

The AP recently ran a story about a substitute teacher who was convicted of exposing students to pornography. Her contention that it was inadvertent because she couldn't keep up with pop-ups seems plausible, but the equally non-tech-savvy jury didn't buy it (despite the fact that the prosecution never even made a reasonable case by checking for spyware). What seems particularly Kafka-esque is the potential 40-year sentence she faces.

<http://www.courant.com/news/local/statewire/hc-14013002.apds.m0230.bc-ct--teacfeb14,0,7509985.story>

✶ The Risks of Updating 80 Year Old Equipment (Re: [RISKS-24.29](#))

<Chuck Weinstock <weinstock@sei.cmu.edu>>

Sun, 25 Feb 2007 21:33:21 -0500

Although the system includes components built 80 years ago, the power outage on Amtrak's Northeast Corridor was caused by a youngster -- a four year old computer system. According to *The New York Times*, 24 Feb 2007, a single command failed to execute on the evening of 23 May 2006, and no one was alerted. The computer system in question apparently reduced power at the substation involved during maintenance and the failed command was to restore the power levels to normal when maintenance was done. The result was a rush hour on May 25th that took down most of the

Northeast
Corridor.

Interestingly the computer that failed was one of a pair designed to provide redundancy. The second computer was out of service at the time of the failure.

It apparently is the case that reducing power during maintenance was unnecessary. When Amtrak asked an unidentified vendor why this was done, they did not have a good explanation. "After the blackout, the equipment manufacturer decided that instead of fixing the system ... the whole procedure should be eliminated..."

``In the old days, you had switches and gauges, and a glance would reveal that one of them was out of position.' ' said William Crosbie, the Amtrak's vice president for operations.

[Edited down from the original article in *The New York Times*, 24 Feb 2007]

<http://www.nytimes.com/2007/02/24/us/24amtrak.html>

🔥 The Risks of Updating 80 Year Old Equipment (Re: [RISKS-24.29](#))

<Jim Geissman <jgeissman@socal.rr.com>>

Fri, 23 Feb 2007 20:31:06 -0800

The key is in the Crosbie quote [last sentence in Chuck Weinstock's excerpt above]. And not at all surprising -- when you're not sure you understand a

technology, you tend to over-engineer and create objects that work forever.

When you think you understand, and are also trying to squeeze every penny

out of the objects, you cut corners (oops, I mean optimize by improving the

design), and then the system may fail wherever your

understanding isn't

correct.

⚡ RFID tracking

<Paul Wallich <pw@panix.com>>

Wed, 21 Feb 2007 13:27:41 -0500

<<http://www.sciencedaily.com/releases/2007/02/070201164742.htm>>

Science Daily: An electronic accountability system developed at Oak Ridge

National Laboratory will result in savings of more than \$2 million per year

at one federal facility alone and will ensure 100 percent accountability of

employees.

[... and so forth ...]

The article mentions the difficulties of making sure RFIDs at a classified

site don't serve as a conduit for leaking information, and claims (among

other things) safety benefits from knowing the locations of all employees

during an emergency (of some kind that miraculously manages not to knock out

any part of the tracking computers or their sensor network, or to damage

anyone's RFID).

As an inventory-control system, it quite possibly makes sense, with the usual caveats. But one does wonder a little about the people-tracking side of it and the possibilities for mischief if any of the reams of generated data got into the wrong hands.

[Also, RISKS readers should always be wary of claims of 100% infallibility. PGN]

✚ Putting the SSN genie back in the bottle?

<Steve Summit <scs@eskimo.com>>
Wed, 28 Feb 2007 22:52:58 -0500

There were several stories in the news today about a delay in implementing new privacy-enhancing legislation in Texas. All SSNs were to have been stricken from publicly-accessible documents, including title records, deeds, tax liens and birth and death records, but in response to complaints that this work could not be completed in time, Attorney General Greg Abbott issued a letter delaying the requirement by 60 days. (See e.g. http://www.weatherforddemocrat.com/homepage/local_story_059145859.html .)

On the one hand this is disappointing, because identity theft is bad, so making SSN's less available is good. But, on second thought, does it even matter any more?

I get the impression that SSN's are so widely available (i.e.,

for just
about everyone in the U.S.) that trying to plug any one
particular hole is
probably all but futile. I found myself wondering (not for the
first time)
what it would take to get U.S. commerce and society to properly
separate the
tasks of identification and authentication. Would federal
legislation
mandating this separation be effective? Would it be even
remotely possible
to get passed? And even if -- somehow -- it were passed, would
it be hated,
because of the seeming "inconvenience" of having to remember and
use secret
authenticators (as opposed to well-known public identifiers)
when performing
transactions that required them?

✉ **Re: DNS roots attacked ([RISKS-24.57](#))**

<Robert Graves <rgraves@ozemail.com.au>>

Fri, 23 Feb 2007 23:12:29 +1100

> ... attacks lasted for hours but passed largely unnoticed by
most computer
> users, a testament to the resiliency of the Internet.

I noticed. I could access some local sites in Australia, but a
number of
major sites such as Google.com.au were completely inaccessible
for me. I
would categorize the Internet as *Severely Damaged* at the time
- but then I
am no expert. Sadly, the thoughts that ran through my mind (and
I'd guess a
number of those other *unnoticing* computer users) were a) why
bother

complaining? and b) to whom to complain? My ISP had no information on its status page about any problems, and my ability to look at other potential information sources was limited by the problem itself. So, I turned the computer off and went to bed. I suspect those quoted "experts" have a vested interest in downplaying the issue.

RISKS? The very nature of the Internet seems to mitigate against "noticing" issues such as this. I just hope that the instabilities of the Internet are resolved before it becomes too critical to our way of life.

✶ Re: DNS roots attacked ([RISKS-24.57](#))

<R A Lichtensteiger <rali@tifosi.com>>
Fri, 23 Feb 2007 16:51:27 -0500

< [See [RISKS-22.32](#) for the attacks that crippled 9 of the 13 root servers in
< Oct 2002. Perhaps the Internet is somewhat more robust now?
PGN]

Certainly the roots are. f.root-servers.net is actually 34 geographically dispersed nodes using IP anycast. The last numbers I have for the other roots says i-root has 13 and j-root has 17 unique nodes.

It's harder to DDoS 34 machines than to do it to one. And the effects will be regionalized. Depending on the distribution of the bots doing the attacking, one or more nodes will be under greater load than others, so some

people will see worse response rates than others.

As the article you cite said, most folks didn't seem to notice the attack.

Redundancy is good for mitigating some risks (keeping this reponse on charter! <g>).

⚡ **Re: DNS roots attacked ([RISKS-24.57](#))**

<Joe St Sauver <joe@oregon.uoregon.edu>>

Wed, 21 Feb 2007 14:12:50 -0800

You mentioned the recent attack on the roots... unfortunately I don't think there's much room to be cheery about the current state of security of the DNS system... if you're interested, see "Port 53 Wars" from the recent Internet2/ESNet Joint Techs session on "Security of the Domain Name System and Thinking About DNSSEC," <http://www.uoregon.edu/~joe/port53wars/> (PPT and PDF formats provided)

⚡ **Re: Crashing an in-flight entertainment system (Summit, [RISKS-24.57](#))**

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

Wed, 21 Feb 2007 14:37:09 PST

[Hugh Thompson's blog continues with further discussion. PGN]
<http://blogs.csoonline.com/node/151>

Submitted by Anonymous on Wed, 2007-02-21 11:25.

Er, Um, avionics software ain't that grand either, if you go by some examples of Airbus software. An Airbus went off the end of a runway a while back, and an investigation revealed:

- * A leetle bit of water froze in a brake cylinder.
- * The brake system software detected the problem, in the secondary brake system. So far so good. The software then:
 - * Did its normal thing, disabled the PRIMARY brake system, the good one.
 - * Put up a misleading error message on an out-of the way display page.
 - * The pilot eventually noticed this error message, so he pressed a button to clear the message.
 - * But he pressed the button for under 50 msec, so one flight control computer saw the press, but the other one didn't.
 - * The computers noticed they disagreed, so one of them shut down.
 - * The pilot noticed the shutdown, so he pressed a "master reset" button.
 - * But as it turns out, the "master reset" button doesn't really, like, reset everything, but it tells you it did.
- * Therefore when they applied the brakes, only the secondary (frozen up) brakes were applied.

* The pilots, used to this super double-redundant computer-controlled brake system, didn't even think to apply the brakes manually.

* Plane went off end of runway, many \$\$\$\$\$\$\$ of damage.

That's just one example of AirBus software wonderfulness.

⚡ Re: Amazing boilerplate in Fairfax County e-mail (Goldberg, [R-24.57](#))

<msb@vex.net (Mark Brader)>

Wed, 21 Feb 2007 16:21:05 -0500 (EST)

> Looks like the "cutting edge" is severing Fairfax from the Internet.

> Being offline would be bad enough, but bouncing e-mail? For three or four

> days? Amazing.

Er, which county-level services is it that are so critical that if they're

unavailable via the Internet over a long weekend it's cause for words like

"hard-to-believe", "amazing", "anger", and "outrage"?

Mark Brader, Toronto, msb@vex.net

⚡ Disposable digital Cameras are truly digital (Re: R-24.52,54,56,57)

<Jason Mechler <jasonmechler@yahoo.com>>

Wed, 21 Feb 2007 11:52:49 -0600

To end recent debate about the existence of disposable digital cameras,
please see the following 2004 article in *Time* magazine. An acquaintance
of mine bought one of these when they first came out and attempted to hack
so it could be reused. A simple google search now pulls up instructions for
converting these phones to multi-use.

Time Article: [http://www.time.com/time/gadget/20040825/Single-to-Multi-Use Hacks](http://www.time.com/time/gadget/20040825/Single-to-Multi-Use-Hacks): <http://www.cexx.org/dakota/>

[Carmakers copy and repeat error almost forever \(McIlroy, RISKS-24.57\)](#)

<msb@vex.net (Mark Brader)>
Wed, 21 Feb 2007 16:20:06 -0500 (EST)

RISKS-16.3, 5 May 1994, contained an account of the shock of being locked

>> locked out automatically after closing the door on a stopped car with
>> the engine running ... The problem was reported for a Chevy ...

No, it was reported for a Buick Century. The same item mentioned a Chevy,
but *its* misfeature was to *unlock* doors automatically, perhaps posing a theft risk.

Mark Brader, Toronto, msb@vex.net

WOTE 2007 CfP

<Josh Benaloh <benaloh@microsoft.com>>

Tue, 27 Feb 2007 17:24:51 -0800

Workshop on Trustworthy Elections (WOTE 2007),
University of Ottawa, Ottawa, CANADA, 20-21 Jun 2007
Call for Papers [due 9 Apr 2007]

Election technologies have been a major concern in recent years with numerous questions raised about current methods. The aim of the workshop is to bring together researchers, policy makers, voting officials, and others whose work relates to electronic voting systems to present, discuss, and evaluate promising technologies and schemes to achieve high assurance of accuracy and privacy in the casting and counting of votes.

Full CfP: <http://research.microsoft.com/CONFERENCES/WOTE2007/>

[Josh is the program chair. General chairs are David Chaum and Ron

Rivest. Past WOTE meetings have been very worthwhile. This one is held

in conjunction with the 7th Workshop on Privacy Enhancing Technologies,

and organized by IAVoSS, the International Association for Voting Systems

Sciences. The emphasis is on cryptographic voting methods.

PGN]

REVIEW: "The Art of Software Security Assessment", Dowd et al.

<Rob Slade <rMslade@shaw.ca>>

Wed, 07 Feb 2007 13:39:41 -0800

Mark Dowd/John McDonald/Justin Schuh

BKTAOSSA.RVW 20061214

"The Art of Software Security Assessment", Mark Dowd/John McDonald/Justin Schuh, 2007, 0-321-44442-6, U\$54.99/C\$68.99

%A Mark Dowd <http://taossa.com/>

%A John McDonald

%A Justin Schuh

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario M3C 2T8

%D 2007

%G 0-321-44442-6

%I Addison-Wesley Publishing Co.

%O U\$54.99/C\$68.99 416-447-5101 fax: 416-443-0948 800-822-6339

%O <http://www.amazon.com/exec/obidos/ASIN/0321444426/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/0321444426/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/0321444426/robsladesin03-20>

%O Audience a- Tech 2 Writing 1 (see revfaq.htm for explanation)

%P 1174 p.

%T "The Art of Software Security Assessment"

One of the important parts of a book proposal is a review of the literature that might be related to your topic, and how your book differs from the competition. The preface states that, unlike other

software security texts, this one doesn't deal with security design

and defensive programming, but concentrates on how to find vulnerabilities. The authors obviously haven't done their homework:

there are a number of books that talk about finding weaknesses and

loopholes in software. There are even books that specialize in finding vulnerabilities in specific types of software, such as the

rather spotty "Database Hacker's Handbook" (cf. BKDBHKHB.RVW) and the much superior "How to Break Web Software" by Andrews and Whittaker (cf. BKHTBWSW.RVW). And most of them seem to be, like this work, directed at consultants, security professionals, developers, and quality assurance people.

"The Art of Software Security Assessment" is somewhat distinctive in being particularly directed to programmers. Thus, readers from the consulting, security, and quality assurance fields who do not have a very strong programming background will probably find themselves at a loss to navigate the maze of coding examples.

Part one is an introduction to software security assessment. Chapter one, on software vulnerability fundamentals, starts with a very verbose definition of "vulnerability" that seems to boil down to the idea that a vulnerability is something that someone can use against you. The authors also propose that problems be examined in terms of design vulnerabilities (this is what some other software development literature describes as flaws), implementation vulnerabilities (bugs), and operational vulnerabilities. (The latter seems to be related to improper requirements specification, or simply use of a program in the wrong situation.) One section runs through the software development life cycle (SDLC) noting the types of problems to be addressed in each phase, but the material is much less useful than that in Gary McGraw's "Software Security: Building Security In" (cf. BKSWSBSI.RVW). A brief

overview of design review is found in chapter two, along with a larger section of miscellaneous security technologies. There is also a more-than-usually helpful explanation of threat modeling using data flow diagrams and attack trees. Some of the material is idiosyncratic: the description of "bait-and-switch" attacks seems to be confused with the birthday attack against hash digests. An unstructured collection of content about vulnerabilities, more security technologies, and network models makes up chapter three. Chapter four titularly talks about the application review process. This medley of ideas about ways to check code will give you some suggestions if you are starting the operation, but there is little in the way of analysis of the recommendations.

Part two turns to software vulnerabilities. Chapter five provides very detailed information about the various types of buffer overflows, although the explanations are not always clear unless you already understand the concepts. Important facts about the means of data representation in the C programming language are listed in chapter six, and the abstractions are applicable to other languages. Chapter seven suggests reviewing code in terms of function, such as separately auditing variable use, procedure calls and returns, and memory allocation. Problems with common string-handling (and therefore text-related) statements in C are discussed in chapter eight, along with the significance of differential handling of not-quite-universal data representations by various languages (this commonly results in

malformed data attacks). Not quite in a separate part to themselves, chapters nine through twelve provide internal details of the UNIX and Windows privilege and permission functions, as well as process handling. Chapter thirteen deals with process state information, primarily concerning various race conditions. Unfortunately, the outlines given are not as helpful as they could be, due to a reliance on code examples at the expense of explanations. The authors would do well to emulate the style adopted by Diomidis Spinellis in "Code Quality: The Open Source Perspective" (cf. BKCQTOSP.RVW) who also stresses the auditing of source code, but provides extensive textual background as well.

Part three looks at software vulnerabilities in practice, although limited to network operations. Chapter fourteen provides details of many of the basic Internet protocols, noting checks that should be made for dangerous conditions. The discussion of firewalls, in chapter fifteen, has oddly little material on application-level proxies (and only tangential mention of circuit-level proxies), concentrating on the examination of packet headers. Miscellaneous attacks, with no readily evident theme, are listed in chapter sixteen. Chapter seventeen details HTTP (HyperText Transfer Protocol) and other Web technologies, catalogues some attacks, and gives a brief set of vulnerability checking guidelines. Various vulnerabilities in Web scripting and programming languages are noted in chapter eighteen.

There is a great deal of valuable information within this volume. However, there isn't sufficient explanatory content for the work to stand as a primer

for beginners, and the lack of structure reduces the utility as a professional reference. The reliance on code examples is reasonable for a work aimed at programmers, but it does limit the audience to that group. In addition, the practical parts of the book, in particular, greatly emphasize Web applications. As it stands, this work has much of value to Web developers and Web software testers, but it could have had much broader application with minor improvements.

copyright Robert M. Slade, 2006 BKTAOSSA.RVW 20061214

rslade@vcn.bc.ca slade@victoria.tc.ca

rslade@computercrime.org

<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

Search RISKS using [swish-e](#)

Volume 24: Issue 59

Tuesday 13 March 2007

Contents

- [Errors down Canada's electronic income tax filing system](#)
[Paul Robinson](#)
- [Mega Millions Mess](#)
[Benjamin Jun](#)
- [PG&E sidesteps \\$38 million bill for daylight-saving patch](#)
[Paul Eggert](#)
- [FDA - DST and Medical Device Safety](#)
[Richard I. Cook](#)
- [Countdown to Confusion](#)
[Babington/Tse via Monty Solomon](#)
- [Insured car wrongly crushed?](#)
[Chris Drewe](#)
- [Two traffic engineers deny hacking into L.A.'s traffic system](#)
[PGN](#)
- [Hackers break into Harrisburgh water system network](#)
[PGN](#)
- [Trailing blank causes e-mail failure](#)
[Richard Karpinski](#)

● [Date arithmetic before 1900](#)

[John Gilliver](#)

● [W2SP: Workshop on Web Security, call for papers](#)

[Dan Wallach](#)

● [Re: REVIEW: "Code Quality: ..."](#)

[Peter Mellor](#)

● [REVIEW: "FISMA Certification and Accreditation Handbook", Laura Taylor](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

✶ Errors down Canada's electronic income tax filing system

<Paul Robinson <Paul@paul-robinson.us>>

Thu, 08 Mar 2007 03:39:41 -0500

An article in the 7 Mar 2007 **Toronto Star** (1) states that due to errors in the electronic filing system, Canada Revenue Agency will be unable to accept any tax filings electronically or corrections to prior filings.

The Agency's electronic systems apparently transposed the birth date and the user's Social Insurance Number (the Canadian equivalent to the U. S. Social Security Number) and thus corrupted all electronic databases.

A reference to the incident in Slashdot (2) states that no returns - not even paper ones - can be accepted, "based returns will be stacking up in the mail room, as returns cannot be filed at all until the problem is fixed." This could be inferred from the first paragraph of the article in the **Star**, which reads "a problem with electronic filing is making it impossible even to submit tax returns to the Canada Revenue

Agency."

The remainder of the article in the *Star* says nothing about their system

for accepting paper returns, only about the on-line and telephone systems.

A check of the taxing authority's website(3) regarding the issue states "We

have temporarily shut down public access to electronic services to ensure

the integrity of taxpayer information." and that "We have now traced the

source of the problem to software maintenance conducted on 4 Mar 2007. We

are currently working to bring all systems back online gradually."

A CRA press release dated March 6 (4) states "Commissioner of the Canada

Revenue Agency (CRA) Michel Dorais today instructed some computer applications related to personal income tax filing to be

temporarily halted."

Mr. Dorais also stated "there is no indication that this situation was

caused by intrusion, hacking, or computer virus", i.e. the agency messed

things up all by their lonesome, they didn't need any help from anyone else.

The press release also says, "These applications include online services

like Efile, Netfile, and My Account. Mr. Dorais said that he instructed that

this preventative measure be taken following indications that CRA computer

systems have run into infrastructure problems. In order to safeguard

existing systems and to maintain the integrity of CRA's taxpayer information

holdings, Mr Dorais ordered tax filing processes halted."

Again, while this may imply that the agency is unable to process all returns

- even ones filed on paper - that is not explicitly stated, e.g. don't get your hopes up that you'll get away with a long delay in filing, considering that Canada's tax deadline is April 30, Canadians have even more time than people here in the U.S.

However, an article in **The Globe and Mail** (5) states that taxpayers "can wait for Netfile to return to service, or they can print their returns and mail them to the CRA" which indicates that the paper-based systems are unaffected.

(1) <http://www.thestar.com/News/article/189175>

(2) <http://it.slashdot.org/article.pl?sid=07/03/08/0417247>

(3) <http://www.cra-arc.gc.ca/agency/updates/eservices-e.html>

(4) <http://www.cra-arc.gc.ca/newsroom/releases/2007/march/nr070306-e.html>

(5) <http://www.theglobeandmail.com/servlet/story/RTGAM.20070307.wtaxes0307/BNStory/Technology/home>

[Also noted by Henry Troup, who noted that 17 of 75 databases were reportedly impacted. PGN]

Mega Millions Mess

<Benjamin Jun <ben@cryptography.com>>

Wed, 07 Mar 2007 10:02:03 -0800

A US networked lottery system was overtaxed by demand and had at least two operational problems:

A record \$370M jackpot in the US "Mega Millions" lottery overwhelmed systems used for tracking lottery purchases and ticket numbers.
<http://edition.cnn.com/2007/US/03/07/megamillions.ap/index.html>

In one state (Ohio), the purchasing system went down 25 minutes before the deadline. In another state (California), they could not confirm by the morning after the draw if there were any winners. Loss of sales revenue is one problem, but the delays in authentication open opportunities for more serious fraud.

Benjamin Jun, Vice President of Technology, Cryptography Research, Inc.

[After California results were finally generated, no new winners were discovered -- leaving the two East-coast winners to split the pot. PGN]

⚡ PG&E sidesteps \$38 million bill for daylight-saving patch

<Paul Eggert <eggert@CS.UCLA.EDU>>

Thu, 01 Mar 2007 16:38:45 -0800

In the 1 Mar 2007 *InformationWeek* Paul McDougall reports that utility giant Pacific Gas & Electric says its meters won't work properly on 11 Mar 2007 because of this year's new daylight-saving rules and that reprogramming them would cost \$38 million. The problem is time-of-use billing, where the end-user rates change depending on time of day.

PG&E has worked around the problem by getting permission from the California Public Utilities Commission to change the cutover times instead of upgrading its meters. For example, from 11 Mar through 31 Mar a peak usage period that would ordinarily end at 6pm will instead end at 5pm to compensate for the meters being off by an hour.

PG&E announced this workaround in April 2006. Presumably the workaround will continue through the life of the existing meters.

The workaround encourages power usage in the 5pm-6pm hour. This undermines a primary justification for the 2007 change to U.S. daylight-saving rules, which is to conserve electricity by shifting consumption from late afternoon to early morning.

Here's a reference:

Paul McDougall, "PG&E Says Patching Meters For An Early Daylight-Saving Time Will Cost \$38 Million", InformationWeek 1 Mar 2007
<<http://www.informationweek.com/news/showArticle.jhtml?articleID=197700487>>

FDA - DST and Medical Device Safety

<"Richard I. Cook" <ri-cook@sbcglobal.net>>
Sat, 03 Mar 2007 10:17:42 -0600

FYI: There are lots of dates in modern medical equipment including DST

changes, leap years, and device dependent dates, e.g. the next required preventive maintenance. The alert was not issued because of a theoretical possibility but because of actual user experience. Just when you thought that Y2K was safely behind you...

Date: Fri, 2 Mar 2007 15:57:45 -0500
From: CDER MEDWATCH LISTSERV
Subject: FDA - MedWatch - Medical Device Safety - Change in Daylight Savings Time May Affect Medical Equipment in Unpredictable Ways

FDA notified healthcare professionals and consumers of the possibility that some medical devices/equipment, hospital networks and associated information technology systems may generate adverse events because of the upcoming change in the start and end dates for Daylight Savings Time (DST), and suggested actions to prevent such occurrences. Medical equipment that uses, creates or records time information about a patient's diagnosis or treatment and has not been updated by the manufacturer, may not work properly when the new DST starts three weeks earlier and ends one week later this year. Medical equipment currently in use was likely made before the DST rules were changed and may cause patient's equipment to register the wrong dates for the start and end of daylight savings time this year. Additionally, if a medical device or medical device network are adversely affected by the new DST date changes, a patient's treatment or diagnostic result could be:

- * incorrectly prescribed
- * provided at the wrong time
- * missed

- * given more than once
- * given for longer or shorter durations than intended
- * incorrectly recorded

Related CDRH release: Unpredictable Events in Medical Equipment due to New

Daylight Savings Time Change: <http://www.fda.gov/cdrh/safety/030107-dst.html>

[Also noted by Paul Eggert:]

<http://www.fda.gov/cdrh/medicaldevicesafety/atp/030107-dst.html>

DST: Countdown to Confusion (Babington/Tse)

<Monty Solomon <monty@roscom.com>>

Sun, 4 Mar 2007 20:53:13 -0500

Perhaps the worst that will happen in millions of offices on the second Monday in March is that caffeine-deprived workers will wonder why their automatic coffeemakers failed to perk on schedule. In less lucky workplaces, however, employees might miss meetings, overbook conference rooms or inaccurately record the time or date of important financial transactions.

For the first time in 20 years, daylight saving time will not start on the first Sunday in April. Instead, it will begin three weeks earlier, at 2 a.m. on the second Sunday in March, the 11th.

Devices from the tiniest BlackBerry to the largest mainframe computer must be updated to ensure their internal clocks "spring forward" by one hour at

the right moment rather than on the old date, which has been written into countless programs. Similarly, they must be reprogrammed to revert to standard time a week later than usual, on Nov. 4. Congress decided in 2005 to expand daylight saving time by four weeks, starting this year, in hopes of conserving energy by pushing more human activity into sunlit hours. ...

[Source: Charles Babington and Tomoeh Murakami Tse Countdown to Confusion:

Daylight Saving Time Comes Early This Year, But Will Your Computer Know When

to Switch?, *The Washington Post*, 3 Mar 2007]

<http://www.washingtonpost.com/wp-dyn/content/article/2007/03/02/AR2007030201346.html>

[Marc Sachs mentioned to me that Kerberos-based systems were subject to

failure on 11 March because of a maximum-permitted 10-minute clock

divergence. PGN]

⚡ Insured car wrongly crushed?

<Chris Drewe <e767pmk@yahoo.co.uk>>

Sat, 24 Feb 2007 22:25:30 +0000

Background: In the UK, motor vehicle details have been stored on the Driver

& Vehicle Licensing Agency (DVLA) computer for decades. This includes a

record that the annual Vehicle Excise Duty ("tax disc") is current. For the

last year or two, the annual vehicle inspection ("MoT test") is captured

on-line as it's done, and insurance companies provide details

for a database of insured vehicles. These allow the police to do real-time road-side checks on passing traffic. Drivers are not required to carry documents with them, but the police can require them to be produced ("a producer") at a police station nominated by the driver within 7 days.

In one case, a car was allegedly towed by police and crushed for having no insurance, despite having a valid policy. There are questions about this case, but here are some general comments on the matter from people at the company where I work:

>> A police statement said: "It is the responsibility of insurance companies, not police forces, to ensure that insurance policy details are updated on the national motor insurance database. When deciding if a car should be towed for insurance or licence violations, officers must show `reasonable belief' that an offence has taken place. "Due to inaccuracies on the motor insurance database officers should not only rely on details held there to constitute `reasonable belief'".

>

> Having been involved in our attempts to keep the motor insurers database up to date with details of the company fleet, I can't say I'm surprised that it's sometimes out of date. It seems totally ridiculous that the police use this as the sole evidence that a vehicle should be towed away.

>

>> Gives you great confidence in the ability of the `authorities' to use databases in the pursuit of their version of justice. Imagine

them using a
>> database covering ID cards, they'd be hauling us off instead
of cars
>> then....
>
> Can't help wondering why the police impounded the car instead
of simply
> issuing a producer. Was there something else dodgy about the
car or the
> driver that we weren't told about?

The idea is the computer says no, the journey ends there. The
police will
not allow you to continue in an uninsured car.

There was something on one of those 'fly on the wall' police
programs that
made me wonder. They stopped someone because the computer said
the car was
untaxed and uninsured and the driver tried to show them an
insurance
certificate. The officers were singularly unimpressed saying
anyone with a
computer can knock up a 'valid' certificate of insurance
preferring to
believe what the database told them. At the end of the program
we were
updated and the driver was insured but his tax was 6 weeks out
of date.

Looks like the (rather familiar) RISKS here are (a) ambiguity as
to what is
regarded as the definitive record -- in this case, computer
database or
paper insurance certificate? -- and (b) how individuals can find
themselves
in trouble for others' errors and omissions, e.g. if your
insurance company
makes a mistake in updating the database. Presumably you could
prove in
court that you have a valid policy, but that's not much good if
you're
detained by police at the side of the road a long way from home.

✦ Two traffic engineers deny hacking into L.A.'s traffic system

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

Fri, 2 Mar 2007 13:01:52 PST

Back in Aug 2006 there was a threat of a strike, which caused Los Angeles officials to restrict access to traffic-control computers. However, beginning on 21 Aug 2006, two traffic engineers were able to access those computers anyway, lengthening the red light cycles on major routes, and allegedly causing massive traffic tie-ups for several days at different intersections (LAX Airport, Studio City, the Glendale Freeway, Little Tokyo, and the L.A. Civic Center). Both men pleaded not guilty to felony charges on 8 Jan 2007. [Source: Sharon Bernstein and Andrew Blankstein, Los Angeles Times, 9 Jan 2007; PGN-ed]
<http://www.latimes.com/news/local/state/la-me-trafficlights9jan09,1,899433.story?coll=la-news-state>

[Clifford Neuman is quoted at the end of the article, saying that there are two primary ways to design computers to guard against malicious activity by insiders, but each can interfere with employees' ability to do their tasks and would probably be prohibitively expensive for the city.]

✶ Hackers break into Harrisburgh water system network

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

Wed, 28 Feb 2007 16:11:17 PST

[Marcus H. Sachs sent this to me at the end of October, but it slipped

through the crack. It is never too late for such items to appear in

RISKS, even though some of them may have been overtaken by other events.]

An infected laptop gave hackers access to computer systems at a Harrisburg, Pennsylvania, water treatment plant. The plant's systems were accessed in early October 2006 after an employee's laptop computer was compromised via the Internet (apparently from abroad), and then used as an entry point to install a computer virus and spyware on the plant's computer system. The FBI was investigating. The motive appears to have been the use of the laptop as a zombie, rather than an attempt to subvert the water system.

However, more serious risks are obvious. [Source: Robert McMillan, Hackers

break into water system network, IDG News Service, 31 Oct 2006; PGN-ed]

<http://www.networkworld.com/news/2006/110106-hackers-break-into-water-system.html>

✶ Trailing blank causes e-mail failure

<Richard Karpinski <dick@cfcl.com>>

Thu, 1 Mar 2007 22:27:53 -0800

When a system of components is under disparate control like the Internet, it only works reliably when everybody plays by the rules. E-Mail behavior is specified in rfc2822 and related documents maintained by the IETF. While I can't find it clearly in that document, the general rule is that you should be liberal in what you accept and strict in what you generate.

Here I report on an e-mail address which fails because of a trailing blank. Notice that it can be difficult to see a blank by the naked eye when it is followed by white space. It should not be there. There should be no space after .COM or .NET in an e-mail address. Still, many e-mail programs make it easy to put one there by mistake. In this case, the Apple Macintosh OS X application Mail happily uses such an address and passes the blank along.

No matter; the next recipient will trim it off and there will be no problem. In my case, the e-mail went to the ISP supported by what used to be Pacific Bell, which became SBC and then became AT&T by further corporate manipulations. They use Yahoo to provide outgoing e-mail service for their DSL customers. Yahoo, too, apparently passes the trailing blank along, presumably to a Domain Name Server. No matter. The DNS will trim off the blank and all will be well.

But no. MAILER-DAEMON@yahoo.com says:
Sorry, I couldn't find any host named bzwebtech.com?. (#5.1.2)
And the mail is returned to the sender.

Perhaps the DNS is actually OK; I can't tell from the messages I get.

Still, I believe that at least Mail and Yahoo are not really playing by the rules.

Now a nitpicker is fully equipped to track such a problem down, at least to the point of discovering the unwanted blank, but other e-mail users may not have the resources and may simply assume that the part to the left of the .COM is in error and give up entirely on reaching that company or person. Too bad, since that introduces unnecessary friction and loss in a vital facility.

Surely Apple and Yahoo are wrong in their treatment of a problem originally caused by my own mistake. If the DNS is also wrong, then we may have more to worry about than I knew. The problem is exacerbated by the lack of any convenient way to report problems to any of those entities.

Richard Karpinski, World Class Nitpicker, 148 Sequoia Circle, Santa Rosa, CA 95401 dick@cfcl.com Home +1 707-546-6760 Cell +1 707-228-9716

🔥 **Date arithmetic before 1900 (Re: Excel, Levine, [RISKS-24.57](#))**

<"Gilliver, John \(\UK\)" <John.Gilliver@baesystems.com>>

Thu, 1 Mar 2007 19:31:40 -0000

> less common to do date arithmetic, and I've never seen anyone doing date

> arithmetic as far back as 1900.

Genealogists -- or the software they use -- does it a lot; the one I use (Brother's Keeper -- somewhat clunky by today's standards, but I have a *lot* of records in it and am not translating it all now! It also is excellent at encouraging you to record *source* and *quality* data for all your data), for example, shows the age of anyone it can (by subtracting birth from death if both are recorded, otherwise birth from today -- and no I don't know what cutoff it imposes). It may do other date calculations too. OK, for giving ages in years, this only has a 1 in (about) 365 chance of giving the wrong answer if there's a day funny around 1900, but I just thought I'd mention it as something which regularly does date calculations "as far back as" 1900.

✶ W2SP: Workshop on Web Security, call for papers

<"Dan Wallach" <dwallach@cs.rice.edu>>
Fri, 9 Mar 2007 11:08:26 -0800

Larry Koved and I are co-chairing a workshop on 24 May 2007 on web security (W2SP) that will be co-located with and following the IEEE Symposium on Security & Privacy in Oakland, CA. We're asking for one-page position papers, and our hope is to attract more industrial participation than you'd otherwise get at an academic conference.

The goal is to bring together researchers and practitioners from academia

and industry to focus on understanding Web 2.0 security and privacy

issues, and establishing new collaborations in these areas.

Position papers are due March 23.

Here's the full CFP:

<http://www.ieee-security.org/Calendar/cfps/cfp-W2SP.html>

Re: REVIEW: "Code Quality: ..." (Slade, [RISKS-24.57](#))

<MellorPeter@aol.com>

Fri, 9 Mar 2007 14:12:40 EST

Review by Rob Slade <rMslade@shaw.ca> of "Code Quality: The Open Source Perspective", Spinellis.

> Nonfunctional requirements (including such
> characteristics as reliability, portability, usability, interoperability,
> adaptability, dependability, and maintainability) are much harder
> to assess, and yet may be more important. [...]
> Chapter one introduces the structure of the text by mapping
> characteristics from the ISO 9126 quality standard to the chapters and
> sections of the book.

ISO/IEC 9126 has now been superseded by a set of standards referred to as SQuaRE, but the new standards are still flawed, in the same way that 9126 was (and are direct derivatives of it).

The problem arose back in 1992 when the joint technical committee (JTC1) set up to ensure compatibility between ISO (International Standards Organisation) and IEC (International Electrotechnical Commission) took on a

life of its own and began to write standards without reference to either of its parent bodies.

In particular, ISO/IEC JTC1/SC7/WG6 began to draft standards (the ISO/IEC 9126 series) on "software quality" in which it misused terms defined by IEC/TC56 (Technical Committee 56: Dependability). In particular, terms such as "reliability", "availability" and "maintainability" were defined as "subcharacteristics" of "software quality" without any regard to the standard definitions of these terms in the field of system dependability. (At the time, the working group responsible had not even heard of the standard definitions as stated in IEC 60050 (191): International Electrotechnical Vocabulary Section 191: Dependability and Quality of Service.)

I would advise anyone who is interested in the dependability of systems (i.e., their reliability, availability and maintainability as correctly defined) to take anything emanating from ISO/IEC JTC1/SC7 (Joint Technical Committee 1, committee on "Software Quality") with a very large pinch of salt.

Peter Mellor (UK Principal Expert on Dependability Terminology, IEC/TC56/WG1: Working Group 1, Definitions of Terms.) +44 (0)20 8459 7669

**⚡ REVIEW: "FISMA Certification and Accreditation Handbook",
Laura Taylor**

<Rob Slade <rMslade@shaw.ca>>

Fri, 09 Mar 2007 11:56:32 -0800

BKFISMAC.RVW 20070113

"FISMA Certification and Accreditation Handbook", Laura Taylor,
2007,

1-59749-116-0, U\$69.95/C\$90.95

%A Laura Taylor

%C 800 Hingham Street, Rockland, MA 02370

%D 2007

%G 1-59749-116-0 978-1-59749-116-7

%I Syngress Media, Inc.

%O U\$69.95/C\$90.95 781-681-5151 fax: 781-681-3585 www.syngress.
com

%O [http://www.amazon.com/exec/obidos/ASIN/1597491160/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/1597491160/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/1597491160/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/1597491160/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/1597491160/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/1597491160/robsladesin03-20)

%O Audience a- Tech 1 Writing 1 (see revfaq.htm for
explanation)

%P 498 p.

%T "FISMA Certification and Accreditation Handbook"

The United States' Federal Information Systems Management Act
mandates

certain standards of information security and controls for US
federal

agencies. It extends to contractors and other sources that
support the

assets of federal government departments. However, it may have
wider

application yet, since it provides a solid basis for security
management,

assessment, and assurance for large corporations as well.

Chapter one looks at definitions of various terms surrounding
security and

controls. It is interesting to note that to the usual

certification

(assessment) and accreditation (acceptance) phases the feds add an

audit/evaluation phase between the two. The National

Information Assurance

Certification and Accreditation Process (NIACAP), National

Institute of

Standards and Technology outline, Defense Information Technology Systems

Certification and Accreditation Process (DITSCAP), and Director of Central

Intelligence Directive 6/3 (DCID 6/3), all directions on how to follow

FISMA, are briefly compared in chapter two. A list of job descriptions, and

a brief outline of general project management steps makes up chapter three.

Chapter four examines components of a certification and accreditation

program, mostly in terms of documentation. Chapter five returns to project

management, with a quick look at the initiation phase. An even shorter

mention of creating a hardware and software inventory is in chapter six.

Chapter seven is nominally about determining the proper level for certification (which is, again, primarily related to the number of documents

produced), but turns into an interesting and valuable outline of information

classification. Much of chapter eight, on self-assessment, is a reprinting

of the NIST 800-26 guideline on that topic. Security awareness and training

is touched on briefly in chapter nine. Chapter ten, on rules of behaviour,

is a terse mix of acceptable use and incident response, but it leads rather

nicely into the longer examination of incident response in chapter eleven.

Chapter twelve lists various types of assessment tools, such as vulnerability scanners and code analyzers. I found the privacy impact

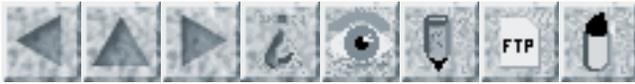
assessment, in chapter thirteen, to be an interesting perspective. Chapter fourteen's material on business risk assessment is concise but reasonable. Business impact assessment, in fifteen, is not quite as good, since it neglects the analysis of criticality of operations. Contingency planning is outlined well in chapter sixteen. Chapter seventeen takes a brief look at risk assessment, but manages to hit all the high points. Change management is reviewed in chapter eighteen. An overview system security plan document is described in chapter nineteen. The certification package is detailed from the perspective of those submitting it (in chapter twenty) and those evaluating or auditing it (chapter twenty-one). Preparation of a plan to correct residual weaknesses is addressed in chapter twenty-two. Chapter twenty-three looks at improving the standings and grading on a Federal Computer Security Report Card.

There is much that is useful and helpful in this book, both in terms of general information security management structure and process, and in terms of references for those involved with FISMA related programs. However, for those who are new to the operation of US government certification and accreditation, the basic requirements, and the relation of the ancillary programs to FISMA itself, could have been more fully explained.

copyright Robert M. Slade, 2007 BKFISMAC.RVW 20070113
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<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

Search RISKS using [swish-e](#)

Volume 24: Issue 60

Friday 16 March 2007

Contents

- ['Embarrassed' Man Sues Microsoft After FBI Finds Sex Videos On His PC](#)
[EEkid](#)
- [Yet more privacy risks from copiers](#)
[Arthur T.](#)
- [Thoughts On New \\$1B Viacom Suit Against Google/YouTube](#)
[Lauren Weinstein](#)
- [Comments on Google's Privacy Announcement](#)
[Lauren Weinstein](#)
- [Yet another risk of voting computers](#)
[Erling Kristiansen](#)
- [When security software goes bad...](#)
[Jeremy Epstein](#)
- [Wireless bingo in UK for smokers](#)
[C R Ritson](#)
- [CBC: Vancouver bus info signs 'duds'](#)
[Andrew Gray](#)
- [Biometric ID at airports](#)
[Peter Mellor](#)

- ['Tamperproof' autopilot for passenger jets to avoid hijacks](#)
[George Michaelson](#)
 - [USAirways Merged Reservation Systems Fubar](#)
[Chuck Weinstock](#)
 - [Re: PG&E sidesteps \\$38 million bill for daylight-saving patch](#)
[Tom Watson](#)
 - [Re: US DST date changes](#)
[Robert Graves](#)
 - [Re: Date arithmetic before 1900](#)
[Ken Hagan](#)
 - [Re: Putting the SSN genie back in the bottle?](#)
[Ketrick McMillin](#)
 - [Announcement: the Ninth Bieleschweig Workshop](#)
[Peter B. Ladkin](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ 'Embarrassed' Man Sues Microsoft After FBI Finds Sex Videos On His PC

<EEkid@aol.com>

March 4, 2007 1:59:35 PM EST

[Via Dave Farber's IP distribution

<http://v2.listbox.com/member/archive/247/@now>]

<http://www.informationweek.com/news/showArticle.jhtml?articleID=197700861>

"Michael Alan Crooker, currently in jail in Connecticut, says security features advertised by Microsoft and its business partners should have kept federal agents from accessing the files on his PC. In court papers filed this week in Massachusetts Superior Court, Crooker says he "suffered great

embarrassment" as a result of Microsoft's failure to keep the FBI's prying eyes off his computer."

"In the court papers, Crooker says he already has reached settlements with Hewlett-Packard, which owns the Compaq brand, and Circuit City."

✈ Yet more privacy risks from copiers

<"Arthur T." <risks.risks.atsjbt@xoxy.net>>

Tue, 13 Mar 2007 16:43:24 -0500

We all know not to leave documents in a shared copier.

A few years ago I found another problem. Someone had tried to copy a page, but the copier didn't have the correct paper. Some time later, when I put in the correct paper, the copier printed out that page that it had remembered. It happened to have been an employee evaluation.

Now, someone has pointed out that most new copiers have hard disks. Even after you've gotten your copy, someone could come along and read what you copied.

Ed McLaughlin, president of Sharp Document Solutions, said about shared copiers: "You actually have a better chance at winning 10 straight rolls of roulette than getting those hard drives on copiers rewritten."

Above abstracted from:

http://p293.news.mud.yahoo.com/s/ap/20070313/ap_on_hi_te/photocopier_risks

[See also May Wong, Photocopies with disk drives may hang on to sensitive data, *San Francisco Chronicle*, 14 Mar 2007, C2]

Thoughts On New \$1B Viacom Suit Against Google/YouTube

<Lauren Weinstein <lauren@vortex.com>>

Wed, 14 Mar 2007 20:15:07 -0700

Greetings. As reported by Reuters:

<http://money.cnn.com/2007/03/13/technology/bc.viacom.youtube.reut>

Viacom has filed a \$1B copyright infringement lawsuit against Google/YouTube.

While this may be viewed (accurately, I believe) in some circles as largely a negotiating ploy, the deeper issues go far beyond that.

My "you can't effectively censor the Internet" postulate suggests that it will always be possible to post virtually any materials, even if this requires "underground" or otherwise obscured communications channels.

However, this is not to say that serious legal and financial risks don't exist related to the YouTube and similar models.

I see two biggies:

First, the obvious one -- regardless of the ability of users to post "offending" materials in other venues, the large services that are most associated in the public mind with the availability of such

items (in this case Google/YouTube) run the greatest risk. This is true both by virtue of their high profile -- they are the natural targets -- but also due to the availability of "deep pockets" for financial settlements or court-ordered payouts.

The second risk is actually even more onerous. I sense an increasing discomfort in the courts regarding the concept of retroactive rather than proactive controls over posted Internet information -- the former is the key basis of DMCA enforcement, of course. This issue doesn't apply only to entertainment-oriented materials, but also to the rising chorus of stories from people who claim (sometimes with validity) that their reputations and lives have been disrupted or damaged by posted online campaigns or false information that they are unable to control or successfully expunge. Over the years, I've head many such stories myself that were sent to me personally, but this issue is rising rapidly in the mainstream media.

The risk here is vast. Courts may choose to upend the current free speech and related DMCA and defamation models, in favor of a much more proactive approach requiring prescreening and total responsibility for all publicly-hosted materials. The impact of such moves would be impossible to overestimate, especially for the larger players in the so-called "Web 2.0" environment. As noted above, these are the very entities who are most likely to be the targets in such situations. Personally, I don't think that

I'd much like the Internet that would result if these sorts of broad government-mandated crackdowns occurred. But the problems are real and do need to be addressed somehow. The laissez-faire approach is reaching a breaking point beyond which the powers-that-be are unlikely to allow it to proceed unaltered.

I believe that there are possible routes to a better situation that could avoid the "doomsday" scenarios. Some of these I've outlined in the past, others I have yet to publicly discuss, but an underlying principle is that the major players need themselves to take more responsibility for the effects of their creations beyond the technical necessities. Better them than the courts and governments I hope you'll agree.

The humorist Tom Lehrer sang: "'Once the rockets are up, who cares where they come down? That's not my department,' says Werner von Braun." -- referring to the German rocket pioneer who both enabled missile attacks on London and was later the father of the U.S. space program.

If officials are able to successfully and publicly paint large Internet corporations as having that sort of attitude, the results could be devastating to the Net. The only ones who can head off this possibility are these firms themselves.

Lauren Weinstein lauren@vortex.com +1 (818) 225-2800 <http://www.pfir.org/lauren>

Founder, CIFIP California Initiative For Internet Privacy <http://www.cifip.org>

Comments on Google's Privacy Announcement

<Lauren Weinstein <lauren@vortex.com>>

Thu, 15 Mar 2007 18:04:40 -0700

Comments on Google's Privacy Announcement
(<http://lauren.vortex.com/archive/000217.html>)

Greetings. Google has announced significant changes to their data retention policy. Since I'm already being asked for my opinion regarding their announcement, I'm sending this out now rather selfishly to avoid having to generate a large number of individual responses (though I'll be glad to discuss this in more depth upon request).

First, the "raw" material:

Google's Press Release:

<http://googleblog.blogspot.com/2007/03/taking-steps-to-further-improve-our.html>

Google's PDF with more details:

http://216.239.57.110/blog_resources/google_log_retention_policy_faq.pdf

Michael Liedtke's AP piece:

http://www.usatoday.com/tech/news/internetprivacy/2007-03-14-google-privacy_N.htm

The gist of the announcement is two changes: The obscuration of some IP address bits (currently it appears that this would involve the least-significant octet of IP addresses recorded in the Google user activity logs), and changes to provide for some form of cookie

anonymization.

Such an IP address change would allow for identification of any one computer out of a group of 256, rather than the existing ability to identify each computer individually. The actual impact of this change from a privacy standpoint would vary greatly depending on the type of addresses (dynamic vs. static) and the total range of those IP addresses associated with any given organization. Cookie anonymization effectiveness is more difficult to analyze until more information regarding the algorithms to be used becomes available.

Both of these changes would be applied to data after an 18-24 month period -- during which time data would be retained intact -- unless future government data retention mandates require longer periods. This is in contrast to Google's policy up to this point of maintaining all log data intact on an indefinite basis.

The AP piece referenced above notes that AOL apparently already goes farther than Google plans to go in terms of IP address anonymization and some other related issues. In light of that, my many public statements over time that have been critical of Google data retention policies, and my "Open Letter to Google: Concepts for a Google Privacy Initiative" from last year (<http://www.vortex.com/google-privacy-initiative>), what is my take right now on this move by Google?

It's much simpler than you might expect. I am not particularly concerned at

this point about the details of the policy. I could (and at some point no doubt will) critique the various aspects of Google's changes in detail regarding both perceived strengths and shortcomings, but not today.

For now, let's view Google's announcement with the broadest possible scope -- not so much for what it says but for what it might portend for the future. While these changes can be reasonably viewed as only a first step on the road to the kinds of data retention privacy enhancements ultimately needed, taking that first step at all is an immensely positive sea change to Google's attitude toward this data.

Time will tell if the rest of that privacy road is traversed in due course. It will be a challenging path indeed, especially in a political environment where the pressure to retain data for extremely broad retroactive investigatory purposes is growing at an alarming rate. And as we've seen in the recent revelations regarding the FBI's violations of the PATRIOT Act (<http://lauren.vortex.com/archive/000215.html>), the issues are all interrelated, and Google of course must obey these laws.

But those are issues for another day. For now, I'll simply thank Google for listening, and express the hope that we can move forward together into a very uncertain future, where deeds will always speak more strongly than words, and where the decisions we make now about these matters are likely to have impacts for generations to come -- as we all ideally try to live by the "Don't be Evil" creed.

It won't be easy. But we have no honorable choice but to try.

Lauren Weinstein +1 (818) 225-2800 Lauren's Blog: <http://lauren.vortex.com>

lauren@vortex.com <http://www.pfir.org/lauren> <http://daythink.vortex.com>

⚡ Yet another risk of voting computers

<Erling Kristiansen <erling.kristiansen@xs4all.nl>>

Thu, 08 Mar 2007 20:58:06 +0100

The election for regional governments (Provinciale staten) in the Netherlands took place yesterday. Many precincts use voting computers, I believe from NEDAP, whose user interface consists of a rather large flat panel with a push-button for each candidate (+ a display and a large "confirm" button, but these are irrelevant here). The layout of the buttons is the same as the layout of the printed candidate list distributed some days before the election. So if you know which button was pushed, you know the candidate voted for.

As is common in large elections, TV news showed a few prominent people casting their vote. Mostly, this is a boring show of people depositing folded pieces of paper in a box. Not this time.

I suppose RISKS readers have already guessed what happened.

Yes, indeed:

The panel was in full view on TV news when the prime minister, the leader of

a main opposition party and one or two other high-ranking politicians cast their votes.

The voting machines have a panel that obstructs the view from the voting officials and the waiting public. But it is completely open towards the side facing away from the public. No privacy cubicles, no curtains, nothing obstructing the view from above. So if one could get away with hiding a camera above the machine, one could record the vote of everybody, and have a picture of the voters as a bonus.

⚡ When security software goes bad...

<Jeremy Epstein <jepstein@webmethods.com>>

Thu, 8 Mar 2007 10:28:42 -0500

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9012499&source=NLT_SEC&nid=38

A bug in Microsoft's new security product (Windows Live OneCare) wipes out Outlook ".pst" and Outlook Express ".dbx" files when it finds malicious email. So it replaces one security problem (the malware) with another (denial of service). Leads to some interesting new forms of attack - send emails to a victim that are just bad enough to trip up OneCare and cause it to launch a DoS attack on its users. Affects Outlook 97 & 2000, and Outlook Express on WinXP.

Shouldn't we have a higher standard for security software in the "do no harm" category? Seems ironic, in particular, that it's a Microsoft product damaging another Microsoft product!

⚡ Wireless bingo in UK for smokers

<"C R Ritson" <c.r.ritson@newcastle.ac.uk>>

Fri, 2 Mar 2007 10:12:30 -0000

I happened to catch a snippet on the radio this morning where two UK bingo-hall operators (who will soon be forced to ban smoking inside) were said to be considering providing customers who smoke with portable bingo-playing handsets to take outside to a smokers' shelter.

I wonder how many risks will be discovered here before and/or after deployment.

Chris Ritson (Computing Officer and School Safety Officer)
Room 707, Claremont Tower, EMAIL: C.R.Ritson@ncl.ac.uk
School of Computing Science, PHONE: +44 191 222 8175
Newcastle University, FAX : +44 191 222 8232
Newcastle upon Tyne, UK NE1 7RU. WEB : <http://www.cs.ncl.ac.uk/>

[I presume those risks will not be smoked out until afterwards. PGN]

⚡ CBC: Vancouver bus info signs 'duds'

<Andrew Gray <agray@alumni.uwaterloo.ca>>

Thu, 08 Mar 2007 12:11:34 -0800

"The signs at the bus stops have been duds," said TransLink spokesman Ken Hardie, adding the company that installed the system said it cannot be fixed.

"This system unfortunately just has never worked properly. Siemens has basically thrown up its hands and say they can't make it work."

<http://www.cbc.ca/canada/british-columbia/story/2007/03/08/bc-signs.html>

Biometric ID at airports

<MellorPeter@aol.com>

Tue, 13 Mar 2007 16:42:23 EDT

The following is from one of my "usually reliable" sources:

- > By the way, I have seen the future of biometric identification and it's
- > here at Quito Airport.

- > Ecuadorians have an index fingerprint on their identity cards. Here at the
- > airport, the biometric check involves the migration officer grasping the
- > ID card in one hand and the subject's index finger in the other, bringing
- > the two together and squinting at them. I shall leave it to you or others
- > to speculate on the accuracy of the system.....

Peter Mellor; Mobile: 07914 045072; +44 (0)20 8459 7669

✈️ **'Tamperproof' autopilot for passenger jets to avoid hijacks**

<George Michaelson <ggm@apnic.net>>

Thu, 8 Mar 2007 12:16:53 +1000

<http://www.thisislondon.co.uk/news/article-23387585-details/New%20autopilot%20will%20make%20another%20911%20impossible/article.do>

I'm sure there are better references. It has potential to be a bottomless pit of falsely raised expectations. At least this is an industry which understands the problem of software testing and things like FCC compliance.

✈️ **USAirways Merged Reservation Systems Fubar**

<Chuck Weinstock <weinstock@conjelco.com>>

Wed, 14 Mar 2007 08:24:06 -0400

[USAirways is in the process of absorbing America West, and merging its reservation systems into SHARES (Shared Reservations System). The following paragraphs have been excerpted by PGN from "Reservations Migration to SHARES. The good, the bad and 'why move to this Reservations system?' "]

We encountered "out of sync reservations," which means that when we migrated the seven million reservations from Sabre to SHARES,

approximately 1.5 million of them didn't "sync up," meaning that

passengers and agents can't do much easily -- like check in for a flight.

The result was that many systems that otherwise were ready to go became

bogged down with lots of these reservations that couldn't be processed

except by hand. By now we've whittled down the number of "out of sync"

reservations closer to a normal level, and continue to reduce them

daily. ...

The short version is this: Much of the technology that most airlines are

built around is "legacy" mainframe systems from the 60's and 70's. These

systems are deeply embedded in everything from reservations, to flight

operations, to airport operations, to accounting. They are very reliable,

but are very inflexible, so as our business changes, we often fight with

one hand tied behind our back. ...

You say: "So dummy, convert it to a 21st century system." We would like to

do that and eventually we will. The biggest reasons we can't do it now are

that there is currently no modern system in use to convert to, and the

investment would be tremendous -- that is, tremendously expensive. Several

companies are building and preparing to implement more modern platforms

for airlines to use and we are watching those closely and are in contact

with those companies. However, even when the opportunity presents itself,

we will have to proceed with caution. In an industry where we lose money

more often than we turn a profit, it's not always easy to

justify

replacing a system that works with a very expensive, untried system that

carries additional risk. But stay tuned; we'll get there.

✈ Re: PG&E sidesteps \$38 million bill for daylight-saving patch (R-24:59)

<"Watson, Tom" <t_wtom@qualcomm.com>>

Wed, 14 Mar 2007 15:45:57 -0700

The original article said:

"...For example, from 11 Mar through 31 Mar a peak usage period that would ordinarily end at 6pm will instead end at 5pm to compensate for the meters being off by an hour."

There is a problem here. According to the PG&E blurb I got (I have a TOU meter), the time period for the interval mentioned is actually 1 hour later (spring forward...). This means that the peak period is actually from 1pm to 7pm (in my case), not 12 Noon to 6pm as it usually is.

The risks: Some people haven't gotten this daylight saving time thing right yet. If errors can be made in our discussions, they can be made EVERYWHERE.

Just to indicate that this has happened before: The clock chip used in the PC/AT (when it was mostly discrete chips) in 1984 used the Motorola MC146818 clock chip. It was HARD WIRED to change daylight saving time on the LAST Sunday of April, and the LAST Sunday of October. The law was

changed to the
FIRST Sunday in April back in 1987 (as I recall, check your time
zone
definitions), and rendered this circuit useless. I don't think
anyone
actually used it anyway. If you are curious, see the datasheet
at:

<http://pdf1.alldatasheet.com/datasheet-pdf/view/122157/MOTOROLA/MC146818D.html>

The description is on page 16, where the 'DSE' (Daylight saving
time enable)
is described.

Legislative note:

The change in 1987 was supposedly at the behest of those who
made barbeques
and the consumables (briquettes). The recent change was made
for "energy
conservation" reasons, but it was mentioned on the news that
since we drive
more these days, it might cause more energy to be consumed.
Time will tell,
and we might go back to some previous "standard". [*]

The political cartoon that went with the first attempt at
changing DST (in
the oil "crisis" of 1973) showed the protagonist cutting a swath
of his
blanket off one end of the blanket and attaching it to the
other. "We call
this daylight saving time...".

Why do we bother with this foolishness. Just have "summer
hours" and
"winter hours". (*SIGH*)

[* A U.C. Berkeley study of Australian energy consumption in
2000/2001

(comparing New South Wales <which extended its DST by two
months> and

Vitoria <which did not>) concluded that energy savings in the
evening

were more than offset by increased energy consumptions in the

morning.

<http://www.nzherald.co.nz/category/story.cfm> 16 Mar 2007

For those of you who shave in the dark under DST, you might do it in the

evening instead, and call it Daylight Shaving Time. PGN]

✉ Re: US DST date changes

<Robert Graves <rgraves@ozemail.com.au>>

Fri, 16 Mar 2007 09:11:10 +1100

In the past (or on Unix machines - take your pick), DST dates were configurable with a simple ruleset. As such, you could define 2nd Sunday in May or 12th February or whatever, the time amount and the designator (AEST, DST etc). A comprehensive default set came with the operating system. This allowed the various DST changes around the world to be *managed* by system administrators, including local anomalies for specific events (such as the Olympic Games in Sydney). Now, we appear to have broken that model, and left it all in the hands of the manufacturers. For example, Microsoft have to release a patch for its OS to cope with the change. Shouldn't it be a simple configuration change? (There is a benefit to the patch - it is simpler, but the patch is the only official way of changing it.) I am very wary of such dependence.

As for all those manufacturers who have embedded fixed rules, it is about time they started reading RISKS and got their act together.

⚡ **Re: Date arithmetic before 1900 (Gilliver, [RISKS-24.59](#))**

<"Ken Hagan" <K.Hagan@thermoteknix.com>>

Fri, 16 Mar 2007 13:18:16 -0000

John Gilliver mentions genealogy software as something which regularly does date calculations "as far back as" 1900.

Yes, and most packages that I've seen also claim to correctly handle the switch from the Julian to the Gregorian calendar, although I suspect that most are assuming the switch-over was 1752. However, I don't think genealogy software counts, because nothing depends on the answers being correct. (My program allows events to precede the birth of the participants. Yes it will warn, but genealogy is not an exact science and good programs don't pretend that it is.)

(Losing the thread somewhat, imagine the mess if there had been computers around in 1752.)

⚡ **Re: Putting the SSN genie back in the bottle? ([RISKS-24.58](#))**

<Ketrick McMillin <ktm5184@ticon.net>>

Fri, 09 Mar 2007 20:36:29 -0600

Steve Summit has accurately observed that Social Security

Numbers (SSNs) are now so widely distributed that efforts by states and the federal government to restrict SSN usage are irrelevant to the problem of ID theft. What's frustrating is that a simple, inexpensive, workable solution is possible but Congress is apparently uninterested.

The solution is to 1) require businesses to report to the Social Security Administration (SSA) the SSNs that have been presented to them, and 2) require the SSA to report to the legitimate holders of those SSNs the identity of those businesses, thus alerting SSN holders to any improper use of their SSNs.

But the SSA can't implement this solution without Congressional action, and members of Congress have shown no interest.

Announcement: the Ninth Bieleeschweig Workshop

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>

Fri, 16 Mar 2007 11:06:50 +0100

The Ninth Bieleeschweig Workshop on Systems Engineering will be held Mon-Tues 14-15 May in the headquarters of Germanischer Lloyd, on the bank of the River Elbe in Hamburg (although I believe the windows in the conference room look to the other side). Participation is free. Germanischer Lloyd has kindly sponsored lunch on both days and dinner on Monday evening. Languages are German and English. The workshops usually attract 30-40

participants

from academia and industry. The Ninth Workshop is organised by myself and Karsten Loer of Germanischer Lloyd, and is, as usual, strongly oriented towards safety-critical systems.

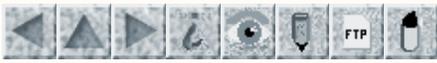
The Bieleschweig series is now in its fifth year, meeting twice a year, with additional meetings (the "half" series) for CausalML and WBA users. They have "themes", and this time we ask for contributions especially in model-based engineering and in incident analysis, although other topics in critical-system engineering are also welcome. The call, timetable, venue details, and some of the planned talks may be found on the Bieleschweig page at the University of Bielefeld: www.rvs.uni-bielefeld.de -> Bieleschweig -> Ninth Workshop.

We publish the slides from the talks, as well as other contributed written material as wished, on the WWW, at the Bieleschweig page at the Technical University of Braunschweig: www.tu-braunschweig.de/ifev/veranstaltungen/bieleschweig and at the Bieleschweig page at the University of Bielefeld www.rvs.uni-bielefeld.de -> Bieleschweig

Peter B. Ladkin, Causalis Limited and University of Bielefeld
www.causalis.com www.rvs.uni-bielefeld.de



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 61

Saturday 31 March 2007

Contents

- [Risks of Virtual Professionalism, Jim Horning](#)
[PGN](#)
 - [Quantum Security](#)
[Rob Slade](#)
 - [Time-handling bug leads to lost time machine](#)
[David](#)
 - [Alaska Government worker formats wrong disks, backups unreadable](#)
[PGN](#)
 - [Latent software risk in aircraft control systems](#)
[Mike Martin](#)
 - [Brazil software ATC failure](#)
[PGN](#)
 - [More railroad-related unintended risks](#)
[PGN](#)
 - [Satellite Navigation may be Hazardous to your Life Of Crime](#)
[Mark Brader](#)
 - [NEDAP, the Dutch chess-playing voting machine](#)
[Mark E. Smith](#)
 - [Typing saves your skin](#)
[Peter B. Ladkin](#)
 - [Proving NON copyright infringement](#)
[Joseph A. Dellinger](#)
 - [A parable about the state of the Web](#)
[Andrew Koenig](#)
 - [Hotel door locks that are too secure](#)
[Kevin Fu](#)
 - [Intuit's Amazing Web Pricing Roulette](#)
[Lauren Weinstein](#)
 - [Re: When security software goes bad...](#)
[Rick Damiani](#)
 - [Two-step authentication](#)
[Marc Auslander](#)
 - [Info on RISKS \(comp.risks\)](#)
-

Risks of Virtual Professionalism, Jim Horning

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

Sun, 1 Apr 2007 00:00:03 GMT

Long-time RISKS contributor Jim Horning has written an outstanding Inside Risks column for the *Communications of the ACM*, 50, 4, April 2007 on *Risks of Virtual Professionalism*. It raises issues of licensing software engineers and of legal jurisdiction on the Internet. Jim is a member of the ACM Committee on Computers and Public Policy (CCPP, the sponsor of the ACM Risks Digest) and has written several previous columns for Inside Risks.

Although I cannot run his article here without violating CACM Copyright, you can find it online for your own personal interest:

<http://www.csl.sri.com/neumann/insiderisks.html#202>

or with accelerated access:

<http://www.csl.sri.com/neumann/insiderisks07.html#202>

Jim's article is the 202nd in the remarkably continuous ongoing monthly series. Previous columns issues are also online:

<http://www.csl.sri.com/neumann/insiderisks.html>

including Jim's April 2004 column:

<http://www.csl.sri.com/neumann/insiderisks.html#166>

Quantum Security

<Rob Slade <rslade@shaw.ca>>

Sun, 1 Apr 2007 00:14:10 -0000

Quantum computing is a field of research based upon the notion of quantum entities known as qubits. Unlike the classical computer bit, which can exist in either a one or zero state, qubits can exist in a superposition of both states simultaneously, and possibly more. This may (or may not) enable us to create new computer architectures which can (or can't) provide new computing capabilities.

The ability for a qubit to hold both one and zero states simultaneously implies that quantum computer architectures will be able to compute all possible|each possible|every possible|all feasible|each feasible|every feasible|all viable|each viable|every viable|all conceivable|each conceivable|every conceivable|all imaginable|each imaginable|every imaginable value for a given problem at once (or not).

Given this new and powerful computer architecture, we may (or may not) be able to perform computations of NP-complete, non-convergent, or least path problems in less than exponential times. This has significant implications for risk analysis and management. Possibly the greatest risk is in pursuing a technology which may never produce a real effect. However, on February 13th of this year, a Canadian company demonstrated a device which is the largest quantum computer built to date (or not).

The superposition factor of computing all possible values holds promise in terms of encryption, but the relation to encryption does not end there. Using the quantum phenomenon of entanglement, the sender can determine whether or not a third party is reading transmissions. (I wonder if anyone is reading this?) Unfortunately, the concepts of quantum encryption, and

quantum computing, although they use different technologies (or not), are entangled in the public mind.

I have, as it happens, been working on a paper (for the next ISMH) on the security implications of quantum computing. At the moment, the paper is in a superposition state of being written and not written. (Until an observer looks at it, have I really written the paper?)

Returning to the topic of risk management, quantum devices may be able to compute, via an assessment of the lowest energy state, the optimum configuration ...

Oh, I'm too tired to finish this off ...

rslade@vcn.bc.ca slade@victoria.tc.ca rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>

Time-handling bug leads to lost time machine

<David <djw@spamcop.net>>
Sun, 1 Apr 2007 00:34:47 -0000

(Inspired by the recent F22 Raptor computer crash crossing the 180-degree longitude...)

I built a working time machine and sent it back to the year 1500. It was supposed to take some pictures. I was planning on retrieving it from 2007 immediately afterwards. Unfortunately, I messed up the code for the Gregorian calendar year adjustment and now I've lost it! Help!

Alaska Government worker formats wrong disks, backups unreadable

<"Peter G. Neumann" <neumann@csl.sri.com>>
Tue, 20 Mar 2007 14:49:52 PDT

A computer technician accidentally wiped out Alaska's huge data file (and the backup disk) containing nine months worth of information on the annual payout from the state fund (reportedly worth \$38 billion) that pays dividends to Alaskans out of the oil revenues. Seventy people had to work overtime for six weeks to re-enter the lost data from 300 boxes of paper. The error cost the state \$220,000 in overtime and consultants. [Source: CNN, 20 Mar 2007; PGN-ed, with thanks to Lauren Weinstein.]

[F. John Reinke also spotted this one (<http://www.msnbc.msn.com/id/17702021/>) and commented:

Gooferment IT at its best. Great design and architecture. How come the only two copies of the data were in the same time zone? Where was security that one "custodian" could access both copies? Where was IT Leadership that had processes and procedures that could fail so miserably? An interesting object lesson. In business, there would be terminations for all involved. FJR

PGN]

✶ Latent software risk in aircraft control systems

<"mike martin" <mke.martn@gmail.com>>

Fri, 16 Mar 2007 11:57:14 +1100

On 1 August 2005, shortly after departing from Perth, Australia, bound for Kuala Lumpur, Malaysia, a Boeing B777-200 passenger aircraft suffered a flight upset while climbing through 38,000 feet. It began when the aircraft spontaneously pitched sharply upward, reaching 41,000 feet and activating stall warnings. After pilots regained control they returned to Perth.

The incident was triggered by a second accelerometer failure in the aircraft's air data inertial reference unit (ADIRU). This unit is designed to be highly redundant and fault-tolerant but the first failed accelerometer's failure mode was not one that had been anticipated during unit design and development. (It had been assumed that a failure would always result in zero voltage output, but this failed device was producing a high output value.) The twin failures exposed a latent software fault, which resulted in the unit feeding incorrect aircraft acceleration data to other flight control systems.

Boeing B777-200 aircraft first entered service in 1995 and this is the first reported instance of the particular software fault, which was apparently present in the unit's original design, affecting operation of an aircraft. The incident highlights the fact that software testing can never eliminate all risk.

The Australian Transport Safety Bureau's investigation report is at

http://www.atsb.gov.au/publications/investigation_reports/2005/AAIR/air200503722.aspx

✶ Brazil software ATC failure

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

Tue, 20 Mar 2007 14:49:52 PDT

The Brasilia air-traffic control center suffered a communications failure (apparently due to software), and a subsequent power failure at the airport, combined with unusually heavy rains. Flights were disrupted over the weekend and on into Tuesday. Earlier outages occurred during the Christmas holidays. (The worst Brazilian air disaster occurred on 29 Sep 2006 when a midair collision killed 154.) [Source: AP item, 19 Mar 2007; PGN-ed]

<http://www.newsday.com/news/nationworld/wire/sns-ap-brazil-flight-delays,0,2571380.story?coll=sns-ap-nationworld-headlines>

✶ More railroad-related unintended risks

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

Thu, 22 Mar 2007 14:11:17 PDT

Here is something sort of similar to last fall's item on flat wheels and

slippery rails ([RISKS-24.47](#),51-53). In this case, locomotives have difficulties reinitializing themselves after the computer system controlling brakes, signals and throttle occasionally lost power. Apparently control signals were arriving out of order. NJ Transit officials attributed the failures to breaking in new engines (PL42s). Reported NJ Transit late train data looks like this:

Year	Delays
2002	400
2003	680
2004	653
2005	732
2006	830

[Source: David A. Michaels, Computer glitches causing delays for NJ Transit, *The Record*, 27 Feb 2007; PGN-ed]

[http://www.northjersey.com/page.php?](http://www.northjersey.com/page.php?gstr=3DeXJpcnk3ZjczN2Y3dnFlZUVFeXk2MDgmZmdiZWw3Zjd2cWVlRUV5eTcwODQ2NjAmeXJpcnk3ZjcxN2Y3dnFlZUVFeXky)

[gstr=3DeXJpcnk3ZjczN2Y3dnFlZUVFeXk2MDgmZmdiZWw3Zjd2cWVlRUV5eTcwODQ2NjAmeXJpcnk3ZjcxN2Y3dnFlZUVFeXky](http://www.northjersey.com/page.php?gstr=3DeXJpcnk3ZjczN2Y3dnFlZUVFeXk2MDgmZmdiZWw3Zjd2cWVlRUV5eTcwODQ2NjAmeXJpcnk3ZjcxN2Y3dnFlZUVFeXky)

An added irony to this is that these trains run to Hoboken, NJ, where Col. Stevens was a pioneer in the development of the steamboat, and by 1825 he had designed the first American-built steam locomotive (on the site of Stevens Institute).

✶ Satellite Navigation may be Hazardous to your Life Of Crime

<msb@vex.net (Mark Brader)>

Tue, 20 Mar 2007 16:09:30 -0400 (EDT)

According to police, a man and a woman stole a Toyota Highlander SUV in the Toronto suburb of Newmarket, planning to drive it to Alberta, but relied on the GPS dashboard device for directions for the trip. It duly gave them the shortest route to Alberta -- one passing south of Lake Huron. So when the license number was routinely checked at the US border, the couple were arrested. Allegedly they were on the approach to the international bridge at Sarnia before they realized it was too late to turn back. A total of four people are now charged in a series of 70 vehicle break-ins in Newmarket in February and March.

(From today's Toronto Star: <http://www.thestar.com/printArticle/193790>)

Mark Brader, Toronto, msb@vex.net

✶ NEDAP, the Dutch chess-playing voting machine (Re: [RISKS-24.60](#))

<"Mark E. Smith" <mymark@gmail.com>>

Fri, 16 Mar 2007 17:59:23 -0700

Erling Kristiansen's submission brought to mind my post entitled, "Wish I'd been wrong department," on Thursday, March 15th, to peoplecount, a hand-counted paper ballots advocates' mailing list:

On 2/24/07, I wrote:

> When you feed ballots into a machine, neither you nor I nor anyone knows
> whether the machine is counting the votes or whether it is playing chess with
> the guy who will feed it the results he wants as soon as all the ballots
> have passed through it.

On page 24 of the April 2007 issue of Harper's magazine, which arrived in my mailbox today, is a little article entitled, "Rooked." It says that a Dutch organization called We Do Not Trust Voting Computers, bought two voting machines to test and found that they were very insecure. They put out a statement saying that one machine was so insecure that it "could just as easily be programmed to play chess as to lie about election results." The machine manufacturer, Nedap, challenged their claim, so the group actually programmed the voting machine to play chess.

***Typing saves your skin**

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>

Thu, 29 Mar 2007 10:54:39 +0200

According to a news item from the U.K. Institution of Engineering and Technology, a team organised by the SANS Institute analysed 7000 detected security vulnerabilities from 1996 (the item says "the 7000" but doesn't say further how they were identified), and found that 85% of them were caused by three phenomena:

- * Failure to check user input
- * Allowing buffer overflows (that is, failing to hinder them)
- * Handling integer type checks or overflows incorrectly

SANS spotted an opportunity and put together a course and practical exam about secure programming, leading to a certificate.

A few observations.

1. Security is not taken as seriously as safety, despite that computer security problems probably cause more total resource damage than accidents. I have long believed, with others, that the phenomena in both areas are similar and thus that similar techniques may be used to assure systems vulnerable to these sorts of phenomena. Devising a threat model is very similar to hazard identification, but whereas hazard identification is partly internationally normed, I suspect that people programming software on networks, especially WWW-based SW, rarely have anything like a professional engineering qualification or status and maybe do not feel as bound to discover and adhere to norms that cover their tasks.

It might help to revise international standards on safety to use the word "dependability" instead of safety, and to use the "specified loss" formulation of the notion of accident rather than the "physical injury or death" formulation, and then security vulnerabilities would be covered. Then again, rather than leading to a higher standard of programming, this might instead just serve to lower the standard of argument for dependability to be found in the required documentation.

2. Working in a strongly-typed programming language would have avoided 85% of the security vulnerabilities discovered (according to some unspecified criteria) in 1996.

It is astonishing to me that 47 years after strong typing was invented and recognised, and after the Turing Award has been presented to such proponents

as Dijkstra, Hoare, Wirth, Dahl, Nygaard and Naur, professionals not using this technology caused 85% of significant errors in a specific area of computing. I think it is disgraceful.

One could always hope that things have changed in the last 10 years. But obviously the SANS Institute doesn't think so.

3. The social phenomena in program construction are overwhelmingly more influential than technical progress. Nothing else could account for phenomenon 2.

<http://www.iee.org/oncomms/sector/informationpro/SectionNews/Object/92520512-96A3-7299-40BC84823F900F5F>

Peter B. Ladkin Causalis Limited and University of Bielefeld
www.causalis.com www.rvs.uni-bielefeld.de

[The SANS of time are measured with geological-scale egg-timers. PGN]

✶ Proving NON copyright infringement

<"Joseph A. Dellinger" <geojoe@freeusp.org>>
Sun, 18 Mar 2007 00:35:39 -0600

Some years ago I created some web pages on geological hazards, being careful to populate them only with photos I actually took myself. No risk of a copyright infringement lawsuit there, right? Wrong!

Over the years, I have been requested several times for permission to use some of my images. I built the web pages for fun, so I always said "sure, just credit me as the photographer, please". Unfortunately, more often than not, when I've later happened to run across one of my photographs (for example, on a geological kiosk on the San Francisco waterfront), I have found that they either failed to credit me, or worse, credited someone else.

Which leads to the risk. A few weeks ago I was told my web pages had been removed at the request of an author of a textbook on geological hazards. An image on my website had clearly been illegally scanned from his textbook. The images were clearly identical. Open and shut case.

Fortunately, the archive.org server showed that the offending image pre-dated the first publication of the textbook. Also fortunately, on the basis of that piece of evidence the author was willing to hear me out, even though he swore he remembered personally taking that photo. He tracked down his original. Turns out it was a "stock" photo provided by his textbook publisher, and they had gotten their copy from... me. Sloppiness in keeping track of who owned what combined with the normal failings of human memory and the passage of time did the rest.

I was lucky in that I had physical evidence to prove I was the original photographer, and my web host and the source of the complaint were both willing to listen to my "implausible" story. And now I will make sure that I keep original unedited source material for anything I make available online, just in case I need to later prove that my site is the source, not the infringer. Non-infringing users of sites like "YouTube" are well advised to do the same!

A parable about the state of the Web

<"Andrew Koenig" <ark@acm.org>>

Mon, 26 Mar 2007 08:10:26 -0400

I was browsing through Yahoo! Finance today and encountered an article with a significant factual error. How significant? Judge for yourself. The article recommended two mutual funds, claiming that one of them "gives you exposure to both large cap and small cap companies." That claim is not true: The fund in question, VEXMX, covers the entire domestic stock market EXCEPT FOR the S&P 500, so it has no large-cap coverage at all. So investors in this fund would get a significantly different risk profile than the article would lead one to believe.

I wanted to send them a correction. So I looked for an e-mail address to use for that purpose. Nothing. But they do let you post comments about the article--at least I can do that.

Not so fast: To post a comment, you must sign in. To sign in, you must have a Yahoo! account. And to get one of those, you have to agree to this:

You are responsible for maintaining the confidentiality of the password and account and are fully responsible for all activities that occur under your password or account.

And this:

You agree to indemnify and hold Yahoo! and its subsidiaries, affiliates, officers, agents, employees, partners and licensors harmless from any claim or demand, including reasonable attorneys' fees, made by any third party due to or arising out of Content you submit, post, transmit or otherwise make available through the Service, your use of the Service, your connection to the Service, your violation of the TOS, or your violation of any rights of another.

And, finally, this:

You and Yahoo! agree to submit to the personal and exclusive jurisdiction of the courts located within the county of Santa Clara, California.

In other words: In order to comment on factually incorrect financial advice given on this website, I have to agree that if anyone steals my password from their service and uses it to do something they shouldn't, and someone sues Yahoo! as a result, then I have to pay both my legal expenses and theirs, and pay any judgment against them if they lose, AND go to California to defend the suit.

Some situations speak for themselves.

Hotel door locks that are too secure

<Kevin Fu <kevinfu@cs.umass.edu>>

Sun, 18 Mar 2007 07:14:43 -0400

During a recent stay at the Best Western in Rockville, MD, a long line

formed at the check-in counter. The desk attendant told me that the new OPERA property management system was just installed earlier in the week, and several problems prevented guests from entering their rooms. Namely:

1. New hotel swipe cards could not be created.
2. The master key was missing.

Problem (1) was apparently on-going throughout the week. To work around the problem, the desk attendant used his master key to let each guest into their room. That is, each guest was escorted to a room and warned that re-entry would require the desk attendant's help. Unfortunately, problem (2) caused complete chaos because now the desk attendant could not open rooms either.

No room keys could be made because after a shift change an employee accidentally took the master key home.

The desk attendant tried multiple master keys to no avail. The desk attendant tried frantically to call the Emergency Services number for the hotel chain, but he only reached voicemail boxes. There were representatives from the company that sold the property management software on site because of the new rollout and employee training, but they were equally helpless without the master key.

A group of roomless customers (including me) gathered in the bar for free drinks. We learned from the bartender that this problem had been going on all week. Whenever the Internet goes down, no one can get room keys or check out (according to the desk clerk). The system is so secure, that the rooms are reserved and yet empty.

One customer in the bar had already checked into his room, but was no longer able to enter because he stepped out for an errand. His medication was locked in his room for several hours, but fortunately lack of medication allowed him to drink beer without complications.

Eventually, the embarrassed desk attendant returned with the master key. The hotel escorted each customer to their room with the master key, but was still unable to create room keys for guests. We were advised to keep one person in the room at all times to ensure re-entry.

As I sit here nursing a tasteless beer, I wonder about the principles for designing a safe and secure property management system. Fail-safe defaults come to mind, as does fault tolerance. A simple DoS attack that disturbs the network would prevent swipe cards from being created. Being secure is nice, but backdoors have their applications.

[This is a write-up of an a-dorable hotel property management system that I encountered last October. -KF]

Kevin Fu, Assistant Professor, Computer Science Department, University of Massachusetts Amherst Ph: 413-545-4006 <http://www.cs.umass.edu/~kevinfu/>

✂ Intuit's Amazing Web Pricing Roulette

<Lauren Weinstein <lauren@vortex.com>>
Fri, 23 Mar 2007 08:32:32 -0700

"Intuit's Amazing Web Pricing Roulette"
(<http://lauren.vortex.com/archive/000218.html>)

Greetings. Earlier this year, on Dave Farber's IP list, I noted my disgust with Intuit's upgrade pricing policy and related customer service discussions -- what I called "Intuit's 'Bait & Switch'" (<http://www.vortex.com/bt/quicken1.txt>) -- which amounted to no discount at all if you only wanted the basic Quicken upgrade.

Now it's time for a much more bizarre installment -- "Intuit's Amazing Web Pricing Roulette" ... and if this ends up looking confusing, that's because it is.

At the present time, depending on exactly how you hit the Intuit Quicken Web site (<http://quicken.intuit.com>), you may be presented with different prices for the same product (in my test cases, Quicken Basic).

In tests so far, I've been offered three different prices:

- \$29.99 (regular retail -- typical store price and what I was originally told was the only available online price whether upgrading or not).
- \$24.89 (with free shipping -- worthless if you download the package -- this one may be difficult to find, so here's proof: <http://www.vortex.com/bp/quicken-firefox.jpg>).
- \$19.99 (the lowest price)

Which of these prices you will see on their Web site appears to depend on a mix of factors. Whether or not you say you are upgrading does not seem to have an effect.

A key issue appears to be your cookie settings.

If your cookies are off, you are likely to see \$29.99. If your cookies are on, you will most likely be offered \$19.99.

In at least some cases, if you try to order at \$29.99 with cookies off, you'll be told to turn cookies on, then you'll see \$19.99 after you've done so. In other cases, you may find \$29.99 (or \$24.89) carried down all the way through the purchase process (here's an example of the high price being used: <http://www.vortex.com/bp/quicken-ie.jpg> .

I am seeing different results depending on the exact sequencing of pages, cookies, and Web browser in use (e.g. Firefox vs. IE).

I have not attempted to delineate all possible permutations or the underlying "rationale" for this behavior, but I would obviously urge extreme caution in dealing with this site.

lauren@vortex.com +1 (818) 225-2800 <http://www.pfir.org/lauren>
Lauren's Blog: <http://lauren.vortex.com> DayThink: <http://daythink.vortex.com>

Re: When security software goes bad...

<"Rick Damiani" <rick@patongroup.com>>
Sat, 17 Mar 2007 16:04:44 -0700

This is actually the re-surfacing of a well known problem with e-mail databases (see Microsoft KB253111, KB262374, KB822158, KB893083, etc.). I

had a similar problem with an older version of Symantec AV running on an exchange 5.5 server. Most of the time it would catch viruses when they showed up in the 'inbound' folder preventing exchange from doing any processing on the infected e-mail. One update added a definition for a virus that had made it through that process and was in the .edb file (exchange's database file), so Symantec AV quarantined it. That crashed the exchange server, with predictable results.

The fix (from Microsoft and Symantec) was to replace the edb file and exclude that folder from processing. Later versions of Symantec added the exclusion on their own. I would say that the root problem is the old Not Invented Here syndrome leading to a failure to learn from history, but MS purchased a (very small) AV company rather than develop an AV tool of their own from scratch. I guess that would be NIH at one remove.

Rick Damiani, Applications Engineer, The Paton Group
California: (310)429-7095 Hawaii: (808)284-3033

Two-step authentication

<"Marc Auslander" <marcausl@optonline.net>>
Fri, 16 Mar 2007 20:42:23 -0400

A silly law has forced many financial institutions to implement two-step authentication. You know how it works. You choose a picture and/or phrase. When you log in, you present your user id, they present the picture/phase warning you to check it, and you then provide a password. Of course, you have to remember a different challenge for each site you use, and remember which ones use this scheme and which don't.

This is not only useless, it's downright dangerous.

It's useless because the average user who's susceptible to phishing is unlikely to notice a missing challenge. Even a sophisticated user is unlikely to notice, IMHO. The naive phishing site isn't going to put up a random picture and tell you to check it, after all. They'll just skip the whole thing and hope you don't notice!

But its worse than that. A sophisticated phishing site could implement a simple man-in-the-middle system. You provide your id, they send it off to your bank, get back the challenge, and show it to you. Now you are really ready to believe you are safe!

Whatever the solution to phishing is, it isn't expecting end users to remember a complicated protocol and notice then its not quite right.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 62

Wednesday 4 April 2007

Contents

- [TJX ID theft: 45.7M and counting ...](#)
[PGN](#)
- [Nothing succeeds like failure](#)
[PGN](#)
- [Risk of depending on a half-used system](#)
[David Lesher](#)
- [Visitor Tagging abandoned for US VISIT](#)
[George Michaelson](#)
- [A couple of unrelated risks](#)
[Jay R. Ashworth](#)
- [Opposition to e-voting grows in France](#)
[Elaine Sciolino via PGN](#)
- [Re: NEDAP, the Dutch chess-playing voting machine](#)
[Debora Weber-Wulff](#)
- [Re: Yet more privacy risks from copiers](#)
[Alistair McDonald](#)
- [Re: 'Tamperproof' autopilot for passenger jets to avoid hijacks](#)
[Rick Damiani](#)

- [Re: Insured car wrongly crushed](#)
[Tony Woolf](#)
 - [AMEX prepaid cards can be forced into overdraft](#)
[Charles Hanes](#)
 - [10TH IEEE High-Assurance Systems Engineering Symposium CFP](#)
[Jicheng Fu](#)
 - [REVIEW: "Botnets: The Killer Web App", Craig A. Schiller et al.](#)
[Rob Slade](#)
 - [REVIEW: "Beyond COSO", Steven J. Root](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ TJX ID theft: 45.7M and counting ...

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

Fri, 30 Mar 2007 9:53:08 PDT

At least 45.7 million credit and debit card numbers from customers in the United States, Britain and Canada were stolen over a period of several years from the computers of TJX. ... The computer breach is significant not only because of its scope but also because the hacker or hackers had access to the decryption tool used to decipher sensitive encrypted information and an ability to intercept data as shoppers' credit transactions were being approved. [1]

Encryption alone is no panacea for threats to consumer data. ... recent details ... show how encryption can be defeated by clever thieves -- and suggest the breach may have been an inside job. [2]

[Sources (PGN-ed):

1. Ellen Nakashima and Ylan Q. Mui, Data Theft Grows To Biggest Ever;

Fraudulent Purchases Pop Up in Breach Of 45.7 Million Shoppers' Records

The Washington Post, 30 Mar 2007

2. TJX breach shows that encryption can be foiled

Ross Kerber, *The Boston Globe*, 31 Mar 2007]

http://www.boston.com/business/globe/articles/2007/03/31/tjx_breach_shows_that_encryption_can_be_foiled/

Nothing succeeds like failure

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

Wed, 4 Apr 2007 11:06:39 PDT

RISKS has included items on some of the largest system development failures.

An article by Shane Harris documents difficulties uncovered by Siobhan

Gorman, going back to the failure of the National Security Agency's \$1.2

billion Trailblazer electronic filtering system development, and continuing

with Turbulence, a new data-sniffing system development that is costing

about half a billion dollars annually and also in trouble. The article also

notes previous development failures of the FBI and IRS. A few excerpts:

"The reasons for these disasters are well-documented and maddeningly

similar: insufficient agency management, contractors that over promised

and anemic-to-nonexistent congressional oversight."

SAIC, the company NSA hired to fix Trailblazer in 2002, was the lead

contractor on the FBI's Virtual Case File [[RISKS-23.89](#) and 24.03].

"And according to its 2006 proxy statement, SAIC is running another NSA

program called ExecuteLocus, which it describes as a successor to

Trailblazer. Out-of-control projects breed more projects ostensibly to right what went wrong."

"Even if they don't know why, there's a reason people keep making the same

mistakes: Failure is one of the most successful things going."

[Source: Shane Harris <sharris@nationaljournal.com>, The Success of Failure,

National Journal, 4 Apr 2007; PGN-ed]

<http://www.govexec.com/dailyfed/0407/040407mm.htm>

⚡ Risk of depending on a half-used system

<"David Lesher" <wb8foz@panix.com>>

Fri, 30 Mar 2007 00:24:34 -0400 (EDT)

'Electronic Medical Records' are one of the latest "Gee Whiz; we aren't

keeping up with the Jones" issue in both private & USG arenas.

Aetna is

even running TV ads hoping you'll surrender all your private medical records

to their database...and whomever gets into it, with or without your permission.

But besides the obvious privacy sacrifice, there's another gotcha. If the

treating hospitals & MD's assume 'the computer knows all' then when it does

not, guess who suffers?

This is not the only article on soldiers who have suffered from the DoD's record-keeping. As part of the *WashPost* series on Army Medical problems, both at Walter Reed and elsewhere, they detailed a soldier with after-effects of an explosive concussion. But when they could not come up with his medical history, they ruled that his depression/PTSD were a pre-enlistment condition, and discharged him sans disability rating.

The RISK? If you put all your data eggs in one basket; the yolks on you if they drop it...

> Disuse of System Is Cited in Gaps in Soldiers Care
> Ian Urbina and Ron Nixon, *The New York Times*, 30 Mar 2007

Lapses in using a digital medical record system for tracking wounded soldiers have led to medical mistakes and delays in care, and have kept thousands of injured troops from getting benefits, according to former defense and military medical officials.

The Defense Department's inability to get all hospitals to use the system has routinely forced thousands of wounded soldiers to endure long waits for treatment, the officials said, and exposed others to needless testing.

Several department officials said the problem may have played a role in the suicide of a soldier last year after he was taken to Fort Lewis in Washington State from Iraq. His intentions to kill himself were clearly documented in his digital medical record from overseas, but

doctors at

Fort Lewis did not consult the file and released him, according to department records and defense officials.

"The D.O.D.'s failure to share data and track patient records is truly a matter of life and death," Senator Patty Murray, Democrat of Washington, said in a statement. "This isn't an isolated case, but a system-wide failure."

Visitor Tagging abandoned for US VISIT

<George Michaelson <ggm@apnic.net>>

Wed, 14 Mar 2007 10:41:23 +1000

http://www.epic.org/alert/EPIC_Alert_14.05.html

"...In a July 2006 report, the Department of Homeland Security's Inspector

General echoed EPIC's concerns, stating that the US-VISIT border security

program fails to protect data collected through the use of RFID tags. The

report found "security vulnerabilities that could be exploited to gain

unauthorized or undetected access to sensitive data" associated with

people who carried the RFID-enabled forms. ..."

but this sentence seems more telling:

"...Essentially, the I-94 form could not guarantee that the person to whom

the form was issued would be the same individual exiting the country with

the form. ..."

Classic instance of "magic tokens" being mistaken for a tightly bound secure outcome, forgetting that who *holds* the magic token probably matters more than whats *in* the magic token.

I'd rather go with tally sticks, or a torn postcard. Actually, if they just tore the I-94 jagged and gave me back half, that would work for me..

✦ A couple of unrelated risks

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

Mon, 19 Mar 2007 14:23:16 -0500

In http://news.com.com/2100-1012_3-6168226.html, the writer notes that Microsoft's new business phone system (where are the Ctrl, Alt, and Delete keys?) will

Rather than [...] multiple buttons for transferring calls and for checking voice mail, [have] a single button [which] will enable users to speak to identify the function they want.

Now, press-to-speak is not quite as bad as "one button for multiple functions" (ask a new BMW owner about iDrive), but "speak the function you want" has -- as has been covered in RISKS before -- its own set of problems... even if you rule out Spider Robinson's famous 'speech-activated

bomb/cub news photog who thinks (aloud) "that'll make a great page-one blow up".' :-)

As usual, though, design by people who don't know what to optimize for is usually a bad thing, and optimizing for training over use (which tends to cast your staff turnover rate into question) is always bad -- ask Allied Van Lines, whose AMS replacement for CAMIS more than tripled their mainframe's load (a 2-transaction CICS process became a 7-transaction one) as well as the staff time to do the work -- or so I was told.

On an unrelated topic, one of the choke points in the food distribution business was illustrated this week by the Great Pet Food Scare of 2006; Ontario based Menu Foods apparently manufactures wet petfood for 17 of the 20 brand names in that market (a fact mentioned, but not explored, by one of the wire-service pieces on the story), and some problem with that food has killed roughly a dozen house pets in the last month.

The waitress who feeds me lunch most days asked me today if I thought that was a low-grade terrorist attack... a thought which some prompt Googling failed to turn up anyone else considering. Hmmm...

Homogeneity, though, is still a bad thing, whether someone's out to get you or not. Concealed original-sourcing can be intrinsically bad too, apparently.

Jay R. Ashworth, Ashworth & Associates, St Petersburg FL USA +1 727 647 1274
<http://baylink.pitas.com> jra@baylink.com

✦ Opposition to e-voting grows in France (Elaine Sciolino via PGN)

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

Wed, 4 Apr 2007 9:27:37 PDT

This is apparently the first French election to use paperless electronic voting systems, although only for about 1.5 million of the 44.5 million voters. Three weeks before the election, Elaine Sciolino reports that many doubts are being raised. One candidate's spokesperson said, "I don't want to lecture America. But we don't want France to fall into the same Kafkaesque balloting as happened in the United States." 80% of the machines will be the Dutch NEDAP (which Ireland used in 2004 and 2006, but has now suspended -- see [RISKS-24.61](#) and the next item below). 160 additional machines will be ES&S-iVotronic (which is the system used in the still-disputed Sarasota election in November 2006), with others being Spain's Indra. Two vendor spins stand out for RISKS readers to chew on:

Matthijs Schippers, director of election systems for NEDAP [see next item]:

"The systems we have developed for France comply with all legal standards and regulations that are incorporated in French electoral law. The accusations have no factual basis."

Rob Palmer, director of marketing and communications for ES&S-iVotronic

"We have an extreme amount of confidence in our machines in France,"

said Rob Palmer, director of marketing and communications for ES&S-iVotronic. "Our machines have proven themselves in thousands of elections in the United States and elsewhere."

[Source: Elaine Sciolino, Opposition to e-voting grows in France, *The New York Times, 4 Apr 2007, A3 in the National Edition; PGN-ed]

✂ Re: NEDAP, the Dutch chess-playing voting machine (Re: [RISKS-24.60](#))

<Debra Weber-Wulff <D.Weber-Wulff@fhtw-berlin.de>>
Sun, 01 Apr 2007 12:34:24 +0200

Mike Smith writes about what is known in Europe as the "NEDAP hack". I had the privilege of seeing Ron Gonggrijp present this at the CCC conference in Berlin in December 2006. I was shocked at the old, simplistic architecture and the easiness of the "hack".

The Dutch group "We don't trust voting computers" reported in February 2007 on a further twist in the story:

(English version:
<http://www.wijvertrouwenstemcomputersniet.nl/English/Groenendaal> :

Voting systems company threatens Dutch state - "Buy my company now or you won't have provincial elections")

It seems that the Dutch government has become entirely dependent on the

insecure and rather outdated NEDAP voting machines. Sensing a good opportunity to make a bit of cash instead of investing in an upgrade, Jan Groenendaal, the owner of the company apparently blackmailed the Dutch government.

Wijvertrouwenstemcomputersniet obtained documents under the Dutch freedom of information act which include an email (English translation: http://www.wijvertrouwenstemcomputersniet.nl/English/Mail_Groenendaal) from Groenendaal to the ministry threatening to quit all work if the government appoints "Hacker" Rop Gonggrijp (the guy who led the chess-playing implementation on the NEDAP computers) to the independent commission for investigating the future of the electoral process, i.e., which software/hardware the government needs to purchase for the next elections.

Groenendaal make an offer the government can't refuse: "The ministry buys the shares of our company at a reasonable price, [...] and we will still cooperate during the next election [the Dutch 2007 provincial elections to be held March 7th]." But the government does not, strangely, snap up the shares offered, so he repeats his "offer", then informs the government that he has told his workers to cease activity "until we have received an answer that is acceptable to us".

The elections were held (if, indeed, they actually were elections) and Wijvertrouwenstemcomputersniet has written to the new minister Ter Horst, calling on her to "take the necessary measures needed to restore confidence

in the electoral process and in the notion that our government can not be blackmailed."

So we have one more risk in the area of eVoting - not some dark, unknown "hacker" throwing the election, but the seller of the hard- or software blackmailing the government because they are helpless to conduct an electronic election without their help.

I vote for paper ballots, anyone with me on this one?

(Sarcastic side note: The German government seems to be considering purchasing NEDAP computers. They are getting a good deal on some used Dutch ones....)

Prof. Dr. Debora Weber-Wulff, FHTW Berlin, Treskowallee 8, 10313 Berlin
+49-30-5019-2320 <http://www.f4.fhtw-berlin.de/people/weberwu/>

✦ Re: Yet more privacy risks from copiers (Arthur, [RISKS-24.60](#))

<Alistair McDonald <alistair@inrevo.com>>

Fri, 16 Mar 2007 21:47:00 +0000

This has been brought up before in [RISKS-22.01](#):
<http://catless.ncl.ac.uk/Risks/22.01.html#subj11>

Alistair McDonald, InRevo Ltd :- <http://www.inrevo.com/>
Author of the SpamAssassin Book (<http://spamassassinbook.packtpub.com/>)

Tel: +44 7017 467 386 (Work) +44 7812 829 020 (Cell)

✶ Re: 'Tamperproof' autopilot for passenger jets to avoid hijacks

<"Rick Damiani" <rick@patongroup.com>>

Sat, 17 Mar 2007 16:22:21 -0700

I'm pretty sure this has come up here before. A quick search of Risks

shows some cautionary tales. I like this one best:

<http://catless.ncl.ac.uk/Risks/24.05.html#subj1.1>

A word from a pilot:

<http://catless.ncl.ac.uk/Risks/24.25.html#subj7.1>

Rick Damiani, Applications Engineer, The Paton Group

California: (310)429-7095 Hawaii: (808)284-3033

✶ Re: Insured car wrongly crushed (Drewe, [RISKS-24.59](#))

<Tony Woolf <news@t-onywoolf.co.uk>>

Wed, 14 Mar 2007 11:01:41 GMT

> ... anyone with a computer can knock up a `valid' certificate of insurance

> preferring to believe what the database told them.

Neither the paper document nor the computer record is proof of insurance.

(A relative found this out the hard way with a surveyor's Professional

Indemnity insurance.) However, both give a reference that allows you to

contact the insurance company and find out whether it is valid.

The police

could have confirmed by phoning the insurance company help line and giving

the car and driver details.

✦ AMEX prepaid cards can be forced into overdraft

<Charles Hanes <chanes@pacbell.net>>

Wed, 4 Apr 2007 13:56:40 -0700

I have been using some prepaid American Express cards that I get through a hotel timeshare program. I just found out something interesting about them.

About 3 weeks after using one of the cards at a hotel in San Francisco, I received a letter from AEIS or American Express Incentive Services, explaining that my prepaid card number was in overdraft by a significant amount. I had directed the hotel to deduct the exact value of the card, and then charge the remainder of the bill to another credit card.

By checking the hotel billing statement, I quickly figured out that the extra amount was not charged to the different card, but was erroneously charged to the same prepaid card number. I was mystified how this was possible.

A complicating factor was that I no longer had the physical card, I unintentionally left it there at the hotel checkout desk instead of bringing it away with me.

So, I called the customer service number on the letter, and explained what

happened. The rep explained that it is possible for a merchant to overcharge the card if they force the transaction, and do not abide by the rejection of the amount. I did not know this could be done.

So, the letter and the representative directed me to mail in a check for the balance, which was no problem since I verified that the amount was valid and did not get charged to the other card.

I asked that the card number be canceled, since I no longer had the card in my possession, and the representative explained that that was automatically done when the card went into overdraft.

Apparently these cards do not automatically cancel when their value goes to zero. The card number apparently remains valid until the card expires. This is very, very dangerous.

Lessons:

- 1) Make certain that only the correct amount gets charged to one of these prepaid cards.
- 2) Do NOT throw it away after you have charged the balance. If someone forces another transaction on the card (and this is possible), the bill comes back to you. Destroy the card securely after you have used up the balance.

<"Jicheng Fu" <jxf024000@utdallas.edu>>

Tue, 3 Apr 2007 11:49:35 -0500

THE 10TH IEEE HIGH ASSURANCE SYSTEMS ENGINEERING SYMPOSIUM
November 14-16, 2007, Dallas, Texas
<http://hase07.utdallas.edu/>

The IEEE International Symposium on High Assurance Systems Engineering is a forum for discussion of systems and software engineering issues to achieve high assurance systems. The focus is on integrated approaches for assuring reliability, availability, integrity, privacy, confidentiality, safety, and real-time of complex systems and the methods for assessing the assurance levels of the systems to a high degree of confidence. Technical and experience papers on algorithms, policies, middleware, tools, and models for high assurance systems development, verification and validation, and assessment are welcome. Papers due by 1 Jun 2007

⚡ REVIEW: "Botnets: The Killer Web App", Craig A. Schiller et al.

<Rob Slade <rmslade@shaw.ca>>

Tue, 03 Apr 2007 11:40:17 -0800

BKBOTNTS.RVW 20070126

"Botnets: The Killer Web App", Craig A. Schiller et al., 2007,
1-59749-135-7, U\$49.95/C\$64.95

%A Craig A. Schiller craigs@pdx.edu

%A Jim Binkley

%A David Harley david.a.harley@gmail.com

%A Gadi Evron ge@linuxbox.org
%A Tony Bradley tony@s3kur3.com
%A Carsten Willems
%A Michael Cross
%C 800 Hingham Street, Rockland, MA 02370
%D 2007
%G 1-59749-135-7 978-1-59749-135-8
%I Syngress Media, Inc.
%O U\$49.95/C\$64.95 781-681-5151 fax: 781-681-3585 www.syngress.com
%O <http://www.amazon.com/exec/obidos/ASIN/1597491357/robsladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/1597491357/robsladesinte-21>
%O <http://www.amazon.ca/exec/obidos/ASIN/1597491357/robsladesin03-20>
%O Audience i Tech 2 Writing 1 (see revfaq.htm for explanation)
%P 464 p.
%T "Botnets: The Killer Web App"

I'm starting the review of this book sitting in the Baker Room at the Microsoft Conference Center, attending ISOI II (the second set of Internet Security Operations and Intelligence meetings). We have just finished singing along with Gadi Evron (who arranged both the community and the meetings) to an Israeli pop song from a few years back (and from a band with the oddly appropriate name of Mashina). Craig Schiller gave me a copy of the book last night at dinner. (When I asked Jim Binkley to autograph it for me he was jealous because he hasn't yet received his own copy.) Carsten Willems was here yesterday, but I haven't seen him to ask him to sign it this morning. I'll have to ask for David Harley's autograph the next time he visits Vancouver.

All of which is by way of saying that it may be difficult to be objective about this book, but ...

The subtitle of chapter one, "A Call to Action," is correct. Normally one would expect a definition of the topic or technology of botnets, but the text is more of an exhortation to pay attention to the problem. The history provided is piecemeal: it does not mention the early DDoS (Distributed Denial of Service) systems (which were application-specific botnets) nor the spambotnet wars of 2004. The definition of botnets in chapter two tends to be technical, rather than functional, and the descriptions and categories could be grouped in a more logical and organized manner. A variety of alternative command and control systems are described in chapter three: the material is well written. The one weakness is the lack of detail on the standard IRC (Internet Relay Chat) control system, but this should probably have been covered more fully in the introductory chapters. Chapter four describes some of the major botnet "client" software families. The content is too technical to be of use to the average computer user, but isn't really all that detailed. Technical information about a variety of possible indications of botnet activity is listed in chapter five.

The use of the Ourmon tool for detecting botnet traffic is discussed in chapters six and seven. (The structure of the text, and the reason for two chapters, is not completely clear, although six is more on installation and seven is more on use.) Ourmon's examination of IRC traffic is covered in

chapter eight. Chapter nine deals with more advanced techniques.

Using the CWSandbox program for malware analysis is examined in chapter ten.

Software tools, research communities, and other sources of information are

listed in chapter eleven. Chapter twelve is a (mostly) philosophical look

at how we, as a society, should respond to botnets. There is also a brief

section on protecting your own computer so as not to become part of the

problem, although assessment and use of a number of the recommendations

would be beyond the capabilities of the average user.

Botnets are a significant problem, and one which has not been adequately

addressed in the current security literature. Therefore, this work is of

major importance. The book does provide a good deal of useful information

for network administrators and security professionals, although better

arrangement of the data and more technical detail would have been even more

helpful. (The brief attempts to address individual users are not successful.) The text is a decent professional reference, and

hopefully it

will promote further attention and activity in this area.

(Security

activity. We don't need any more botnet activity.)

copyright Robert M. Slade, 2007 BKBOTNTS.RVW 20070126

rslade@vcn.bc.ca slade@victoria.tc.ca

rslade@computercrime.org

<http://victoria.tc.ca/techrev/rms.htm>

REVIEW: "Beyond COSO", Steven J. Root

<Rob Slade <rmslade@shaw.ca>>

Thu, 29 Mar 2007 08:58:36 -0800

BKBECOSO.RVW 20070218

"Beyond COSO", Steven J. Root, 1998, 0-471-39112-3, U\$65.00/C
\$84.99

%A Steven J. Root

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 1998

%G 0-471-39112-3

%I John Wiley & Sons, Inc.

%O U\$65.00/C\$84.99 416-236-4433 fax: 416-236-4448

%O [http://www.amazon.com/exec/obidos/ASIN/0471391123/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0471391123/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/0471391123/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0471391123/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/0471391123/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0471391123/robsladesin03-20)

%O Audience i Tech 1 Writing 2 (see revfaq.htm for explanation)

%P 340 p.

%T "Beyond COSO: Internal Control to Enhance Corporate
Governance"

In the preface, the author notes that it is impossible to have complete control of any situation: problems and fraud will happen despite all of our efforts. Root recommends that companies should implement internal controls as suggested by COSO (the Committee of Sponsoring Organizations of the Treadway Commission), but must also go beyond them, in a manner similar to the layered defence or defence in depth models.

Chapter one contains an analysis of the limitations of the COSO directives (and ends with a rather odd overview of the book itself). The concepts of, and problems with, internal control is covered in chapter two.

Chapter

three presents a history of twentieth century corporate frauds and the attempts to restrict them. Business ethics and values are discussed in chapter four.

Chapter five outlines the COSO framework, noting that internal controls provide assurance of the efficiency of operations and reliability of financial reporting--as long as there is compliance with the laws and regulations. (As this material is based on the 1992 version of COSO, it is interesting to note that the components of risk management are pretty much the same, but that the dimensions of objectives categories and unit-levels had not yet been added to the model.) Further concerns and limitations of COSO are expressed and analyzed. Additional frameworks are reviewed in chapter six. Using a hybrid of devices from these other frameworks, chapter seven suggests the extension of internal controls with additional management aspects. Chapter eight recommends that an oversight process be established for internal controls, noting particularly legal obligations and related factors such as standards of care, generic corporate organization and business roles and tasks. The oversight issues are extended in chapter nine, looking in more detail at job roles, and also insights that arise from chaos theory. Chapter ten finishes off the book with a review of the reporting of internal controls: much of this is concerned with the wording used in such statements, and the ineffectiveness of such reports to control

incidents and fraud.

Despite its age, this book is one of the more useful guides in the area of governance and controls in corporations. Root was willing to go beyond the usual promotional jobs that masquerade as management advice. While he does not solve the problem, he at least makes the issues clearer, and raises interesting points in regard to solutions.

copyright Robert M. Slade, 2007 BKBECOSO.RVW 20070218
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<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

Search RISKS using [swish-e](#)

Volume 24: Issue 63

Sunday 15 April 2007

Contents

- [Mars Global Surveyor review panel](#)
[PGN](#)
- [Boy falsely jailed because of DST changeover](#)
[Ron Garret](#)
- [Caltrain *Double* Daylight Time](#)
[PGN](#)
- [Computerized Voting machines](#)
[Arthur J. Byrnes](#)
- [Washington DC Metro replacing software that causes fires](#)
[Jeremy Epstein](#)
- [When banking real time isn't really real time](#)
[John Pettitt](#)
- [Surely it can't be this easy?](#)
[Ted M Lee](#)
- [On "proving NON copyright infringement"](#)
[Ferdinand J. Reinke](#)
- [A Botted Fortune 500 a Day](#)
[Gadi Evron](#)

- [Airline Online Payment Requires Citizenship No.](#)
[Chris Brady](#)
 - [Re: Insured car wrongly crushed?](#)
[David W. Brunberg](#)
 - [Reminder - Computers, Freedom & Privacy 2007](#)
[Stephanie Perrin](#)
 - [Joint HCMDSS and MD PNP: EXTENDED ABSTRACT DEADLINE 20 Apr 2007](#)
[Steve Goddard](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Mars Global Surveyor review panel

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

Sat, 14 Apr 2007 11:54:05 PDT

The review board has concluded that an errant computer command five months earlier had been placed in the wrong memory location, which acted as a time bomb that effectively disabled a safety feature intended to keep the solar panels from rotating too far, ultimately hindering communications. In its final 13 minutes, Global Surveyor reported various alarms. In attempting to recover, the sun-oriented battery overheated, the resulting signal was misinterpreted by the software, which stopped charging the OTHER battery.

Because of the earlier error, controllers could no longer control the spacecraft. Launched in 1996, and taking 10 months to reach Mars, Global Surveyor sent back 240,000 images, lsating much longer than originally intended. [Source: Kenneth Chang, *The New York Times*, 14 Apr 2007; PGN-ed]

🔥 Boy falsely jailed because of DST changeover

<Ron Garret>

Sat, 7 Apr 2007 10:44:57 -0700

[http://www.passablynews.com/index.php?subaction=showfull&id=1175830780&archive=&start_from=&ucat=&](http://www.passablynews.com/index.php?subaction=showfull&id=1175830780&archive=&start_from=&ucat=)

In a nutshell: on 11 Mar 2007, a school received a bomb threat and through their phone logs traced the call back to a 15-year-old boy, who was arrested and incarcerated for twelve days despite the fact that the boy's voice sounded nothing like the voice on the tape.

Of course the authorities had forgotten about the early onset of daylight savings time, and the boy had actually called the school *an hour before* the bomb threat.

Aside from the scary fact that it took twelve days for the authorities to sort this out, the account contains this precious little burn-the-witch moment:

"After he protested his innocence, ... the principal said: 'Well, why should we believe you? You're a [terrorist]. [Terrorist]s lie all the time.' "

All this would be more amusing if we hadn't been doing more or less the same thing on an epic scale for over five years now.

✂ Caltrain *Double* Daylight Time

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

Thu, 5 Apr 2007 11:26:41 PDT

During the week beginning with April Fools' Day, the Caltrain time display has been one hour **ahead** of PDT. I presume that a manual change was inserted at the time of the US cutover to DST, and that the subsequent preprogrammed change was not disabled. It is utterly amazing how complicated clock arithmetic management seems to be for developers and users.

✂ Computerized Voting machines

<"Arthur J. Byrnes" <ajb1@ajb.com>>

Thu, 05 Apr 2007 14:43:53 -0400

Here in Florida, the voting screw-up capital of the world, our legislatures are being bombarded by both "sides" of the voting machine debate.

Amazingly, there is a well funded and vocal group that doesn't care about voting integrity, and are working to convince the legislature that the lack of touch screen machines is an infringement on the rights of the disabled.

[*] Their logic is that since the disabled (usually blind or physically impaired) folks cannot enter the polling place and cast their vote without

some extra help, that their voting rights are being denied.

Their quote is

at the end of this article;

<http://www.news-journalonline.com/NewsJournalOnline/News/Politics/LocalGov/evlHEAD01POL032107.htm>

The folks looking for a paper trail are considered the enemy of the disabled

since there is not yet a certified touch screen machine with a paper trail, in Florida.

Worse yet, there is a subset of folks who have latched onto the paper trail

fight who erroneously believe that the voter will get a copy of the

submitted paper, so that they can verify that the vote they cast, was

properly recorded. In my communications with these folks, I have found that

the vote buying that could occur, never crossed their mind.

The sad part about all this is that the lobby for the disabled has stated

that they don't care about the integrity of the system, and that their only

goal is to make sure that there members can vote. During the time that this

debate was at its peak, they had many of their members from out of state,

call Florida radio talk shows, using pre-scripted speeches, stating that

they felt that their voting rights were being limited. Luckily, there

members were honest, (even if their lobbyists are not) and when asked where

they were located, and if they ever voted in Florida, would answer

truthfully. (Radio talk shows are the grass roots leaders in many parts of

Florida.)

Almost no one in politics has enough understanding of the

technology to see
the pit falls of a virtual voting system. And almost no
politician has the
backbone to stand up against a lobby claiming to be helping
disabled folks.

It is hard to understand, especially in a state that is forever
tainted by
the largest election upset in recent US history, why any
resident would even
consider a system that has questionable output, that is not
recountable.

(The paper votes from the 2000 election were each recounted, by
an
independent group of Newspapers, and the results were correct,
but that was
not front page news...)

Greetings from Flori-duh, Arthur

[* Actually, there are also some very articulate statements
from within

the visually impaired community that counter this argument,
for example,

Noel Runyan's report, "Improving Access to Voting"; see www.demos.org and

www.voteraction.org . Noel is exceptionally well qualified in
this

regard: "Noel Runyan became a critic of voting machines after
his own

experience with the Sequoia Edge II and subsequently became an
expert

witness in three separate lawsuits brought by Voter Action
alleging that

the machines were inadequate and therefore unlawful. He has
worked with

advocates to promote accessibility and security in voting
systems as

mutually attainable goals." PGN]

Washington DC Metro replacing software that causes fires

<Jeremy Epstein <jepstein@webmethods.com>>

Sat, 14 Apr 2007 07:35:47 -0400

This is certainly not the only case of software causing a physical problem, but it's one of the more unusual ones I've run across.

Metro (Washington DC's subway system) is one of the more automated subway systems around. The key to the problem seems to be as follows: "The fire [on Easter Sunday] started after a sensor underneath the rail car failed, causing the voltage in the car to rise. At the same time, the software designed to monitor the flow of electricity also failed, causing overheating in the resistor grid, an electrical component under the car that absorbs excess energy, officials said. A Metro official said the software was not designed to take into account the failure of the voltage sensor. A check of all affected rail cars found no other bad sensors, officials said."

As I've been spending a lot of time working on electronic voting issues, I thought about how a few simple word changes might explain some of the voting system failures we've seen - perhaps failures of sensors on touch screens are causing unexpected interactions. This is just an hypothesis - but shows that just as Metro undoubtedly spent millions of dollars testing the rail cars without finding this problem (until a serious fire brought it to their attention), so too might similar problems occur in voting systems. The

difference is that in today's paperless voting systems, the fire is smoldering quietly and unseen - but still doing damage.

http://www.washingtonpost.com/wp-dyn/content/article/2007/04/12/AR2007041202061_pf.html

✦ When banking real time isn't really real time

<John Pettitt <jpp@cloudview.com>>

Thu, 05 Apr 2007 01:07:42 -0700

A friend of mine had an interesting banking experience with Citibank this weekend. She wrote a check for \$990 on Friday expecting it to take at least two days to clear. On Saturday she was surprised to see a negative \$300 balance. No problem, she transferred \$1500 from another account at the same bank via an ATM. A subsequent check on line later that day showed the new money in her account, a positive balance and the universe back in harmony. Then things got weird. On Monday Citibank credited back the \$990 check as a returned check and debited a \$30 fee for doing it. The end of day balance for Monday was over \$2200.

We both went into the branch today, and the manager couldn't give a rational explanation as to how a check that appeared to have cleared in real time and caused an overdraft (for which they charged interest) had in fact not cleared and how a \$1500 transfer that was available in real time (she took

some of it out at an ATM which also showed the check as cleared) was now only showing as credited on Monday. As best I can figure out the system only appears to effect transfers and clear checks in real time when, in fact it's still happening on an end of business day basis.

The result is what you see on the screen is not really what you get. The manager credited the \$30 and my friend smoothed things over with the recipient of the bounced check but I will now be much more skeptical of what Citibank's computer is saying to me.

John Pettitt (who in another life wrote credit card processing software)

✶ Surely it can't be this easy?

<Ted M Lee <ted.lee@baesystems.com>>

Thu, 5 Apr 2007 14:30:52 -0500

I just returned home from staying at hotel, part of a major chain I won't embarrass by naming. It uses one of the now almost ubiquitous mag-stripe room keys. I returned to my room the second day and discovered the key wasn't working. I walked over to a nearby house phone and called the front desk to report my trouble. The clerk apologized for whatever trouble I was having and promised to send a new key right up. She then started to say something about my cell phone and I thought maybe she wanted to be able to call me back and then I realized she'd been asking if I'd

carried the key
next to my phone. (yes, I had been -- I gather now that's an
easy way to
erase them.) Apart from that useful piece of information which
I'd probably
read before but never noticed (since I only recently joined the
21st century
and got a cellphone) that's not the point. I waited awhile and
somebody did
show up and handed me a new key -- I did give him my old one,
although he
didn't ask for it. Nowhere in any of this process did anyone
ask for any
identification -- I'm not even sure I identified myself when I
called the
front desk. Need I say any more?

✈ **On "proving NON copyright infringement" (Re: Dellinger, [RISKS-24.61](#))**

<"r @ reinke" <reinke@reinke.cc>>
Sun, 1 Apr 2007 09:50:17 -0400

This sounds like a case for "watermarking", "stenography", or a
good old
fashioned notary?

I am surprised that the concept of a "digital notary" has not
taken off for
just such situations. (Maybe there's a web20 application for me
make into
the next google? I could be rich! And, get a life, instead of
reading
ezines, blogging, and commenting.) Maybe it has and I just
haven't heard of
it!

While the Internet Archive is a good idea, one has to wonder if

push came to
shove (i.e., think RIAA as the model for a Pyrrhic victory) if
that would be
acceptable evidence in a legal proceeding.

I'd envision the digital notary as a website that:

CASE#1 -- takes an url, "photographs" it, computers a digital
signature,
saves and encrypted copy, sends you a receipt, and publishes the
checksums.

The disadvantage is that you have exposed your content on the
web.

CASE#2 -- takes anything you send it and do the same. The
disadvantage is
you've shown it to a nosy notary like me.

CASE#3 -- takes a file from you that you want to keep secret and
"seals" it
as well in a similar fashion.

[NOTE: I need two key pairs. Call them FERDINAND and REINKE. I'd
envision
that I'd take my secret treasure map (MAP) to the Lost Treasure
of the
Sierra Madre and encrypt it with my REINKE private key.
WORK1=ENCRYPT(MAP,REINKEPRIVATE) Anyone who had that file could
read the map
using REINKEPUBLIC. Then, I'd encrypt it with my FERDINAND
private key.
WORK2=(WORK1,FERDINANDPRIVATE) Anyone who had this file would
know there was
a file and it was mine by using FERDINANDPUBLIC. Then, WORK2
goes to the
notary. The notary decrypts WORK2 with FERDINANDPUBLIC, and
ENCRYPTS with
NOTARYPRIVATE and returns it to me. Then, since I am getting old
I promptly
forget all my passwords, lose the keys, and the LOST TREASURE
stays lost.]

The digital notary would seem to be a useful service for such

disputes.

Now all I need is a PowerPoint deck and some VCs. And a spare checkbook to put all the money in.

Ferdinand J. Reinke, Kendall Park, NJ 08824 <http://www.reinke.cc/>
blog: <http://www.reinkefaceslife.com/>

⚡ A Botted Fortune 500 a Day

<Gadi Evron <ge@linuxbox.org>>
Thu, 12 Apr 2007 05:45:01 -0500 (CDT)

Support Intelligence releases daily reports on different fortune 500 companies which are heavily affected by the botnet problem, with many compromised machines on their networks.

You can find more information on their blog:
<http://blog.support-intelligence.com/>

They are good people, and they know botnets.

⚡ Airline Online Payment Requires Citizenship No.

<"CJB" <chrisjbrady@gmail.com>>
10 Apr 2007 06:18:38 -0700

Recently I was trying to book an internal flight on Brazilian airline TAM, I made my ebooking OK, and then went on to the VISA payment stage (not via

PayPal). I typed in my country address as UK. It also wanted my date of birth. All OK so far. But then it also wanted a CPF number. I phoned VISA (on a premium rate phone no.) and after being on hold for a long while, a call agent then admitted that she hadn't a clue what a CPF no. was. A search of the newgroups elicited that this was a Brazilian citizenship no. for tax and social security purposes. I obviously did not have such a no. And so TAM lost its online booking. Time wasted - one hour.

The TAM web site was stupid enough to think that just because I wanted to book a flight online that I was a Brazilian citizen not a tourist from the UK.

The risk? Due to the poor design of its booking and payment system TAM lost an online booking for the want of an 11-digit no. which I did not have. I wonder how many other online bookings it has lost because of this?

⚡ Re: Insured car wrongly crushed? (Drewe, [RISKS-24.59](#))

<David W. Brunberg <dbrunberg@firstenergycorp.com>>

Thu, 5 Apr 2007 07:41:29 -0400

I apologize in advance for the (perhaps overly, but not completely for this situation) detailed nature of this submission. I've tried to edit it as best I can to keep the content strictly relevant.

They stopped someone because the computer said the car was untaxed and uninsured and the driver tried to show them an insurance certificate. ...

Looks as if the (rather familiar) risks here are (a) ambiguity as to what is regarded as the definitive record -- in this case, computer database or paper insurance certificate? -- and (b) how individuals can find themselves in trouble for others' errors and omissions, e.g. if your insurance company makes a mistake in updating the database. Presumably you could prove in court that you have a valid policy, but that's not much good if you're detained by police at the side of the road a long way from home.

I can think of an analog situation in the U.S. that, while it admittedly affects a much smaller group of people, is far scarier in terms of its potential consequences. Under U.S. law (and few other than a rarefied group of collectors know this), it is legal to own certain rare and exotic small arms such as machine guns and firearm sound suppressors if properly registered. The Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATFE) is charged by the National Firearms Act of 1934, as amended (NFA), with maintaining the National Firearms Registry and Transaction Record (NFRTR). In short, all transfers of such firearms (to and between licensed dealers/manufacturers, individuals, law enforcement agencies, and corporations) are subject to a tax (waived in the case of government agencies and licensees), recording in the NFRTR, and in the case of individuals, very stringent background checks. Military organizations are

the only entities exempt from these recording requirements. As an aside--and the reason for this will soon be demonstrated--collectors of NFA items are typically very detail-oriented when it comes to strict adherence to the law.

When an individual transfer is initiated, the transferor and transferee fill out a paper document known as a Form 5320.4 (there are other forms and situations but I'm trying to keep this simple--the law sure doesn't) and submit it in duplicate , along with payment of the transfer tax, to the ATFE's NFA Branch, which investigates the item's history, if any, in the NFRTR. Upon successful completion of the necessary background checks, the ATFE approves the Form 4, updates the electronic NFRTR, and affixes and cancels a Tax Stamp bearing the item's serial number to each original paper document. ATF then keeps one original for government records and sends the other to the transferor, who gives it to the transferee, along with the firearm in question.

As has been reported elsewhere,

<http://www.cs.cmu.edu/afs/cs.cmu.edu/user/wbardwel/public/nfalist/rip/index.html>

the NFRTR has been in deplorable condition for some time. Many registration documents have been lost by ATFE, and some were even willfully destroyed by ATFE contract employees in a well documented case. Furthermore, the electronic database that serves as the authoritative Registry is known to have serious flaws and inconsistencies. Due to various political and

financial issues, the ATFE has been slow to rectify these problems with the NFRTR (although the pace seems to have picked up since a recent wholesale relocation and restaffing of the NFA Branch). Thomas Busey, who was the Chief of the NFA Branch for a period in the 1990s, admitted in a videotaped training session in 1995 that the NFRTR had a 49-50% error rate. Mr. Busey also stated in this session,

"Let me say when we testify in court, we testify that the data base is 100 percent accurate. That's what we testify to, and we will always testify to that. As you probably well know, that may not be 100 percent true."

In a 1998 letter to Chairman Dan Burton of the House Committee on Government Reform and Oversight

http://www.cs.cmu.edu/afs/cs.cmu.edu/user/wbardwel/public/nfalist/rip/leasure_letter_re_nfa_destruction.txt

pursuant to a conviction based on flawed NFRTR information, David Montague, an attorney for the defendant (whose convictions were previously overturned) wrote:

"To make matters worse, Mr. Busey was summarily fired and the transcript of his remarks hushed up. His remarks did not become known to the world until obtained on an FOIA request from attorney James Jeffries, III, of Greensboro, N.C."

Given the steep penalties for mere possession of an unregistered firearm regulated under the NFA (minimum sentence: up to 10 years' imprisonment and/or a fine of \$10,000 for each violation), there is a high RISK to lawful

transferees associated with the poor condition of the NFRTR brought about by neglect and/or willful violation of the law by the government agency charged with upholding this law.

Thankfully, it is considered an affirmative defense for a person found in possession of an NFA-regulated item to produce their original approved registration document, complete with canceled tax stamp. This typically is enough to prevent any further legal action against the individual, presuming no other laws have been violated. However, it's no excuse for an agency not maintaining a correct record.

Otherwise, as James Bardwell, a documentor of firearms law, and keeper of the NFA FAQ states:

http://www.cs.cmu.edu/afs/cs.cmu.edu/user/wbardwel/public/nfalist/nfa_faq.txt

"If you don't have the paperwork, and it isn't in ATF's computer, (it is likely they will check, even though they don't have to prove non-registration, they don't want someone to wave a registration form in their face during a trial) you can have a serious problem."

The RISKS? Having a government registry of items (cars, guns, whatever) that is inadequately maintained, poorly transcribed from paper to electronic database, and considered to be authoritative, without adequate assurance of accuracy. Potentially forcing, due to political realities, government agents to perjure themselves in court when questioned about the accuracy of the records in question. Endangering, by rendering government records

unworthy of trust in court, legitimate cases against truly guilty defendants. In the special case of the UK's auto registry, the lack of recourse "at the curb" to paper documentation by the defendant is unnecessary and injurious. In any event, regardless of the stakes or whether the individual is innocent of wrongdoing, it can be prohibitively expensive (in time, money, reputation, and opportunity cost) to defend oneself when the big wheels start turning. And it seems especially unjust when the situation is initiated by "others' errors and omissions"--much less their willful violation of the law.

Reminder - Computers, Freedom & Privacy 2007

<announce@cfp.acm.org>

14 Apr 2007 23:17:03 -0400

Debate the Future at the 17th annual Computers Freedom and Privacy Conference, 1-4 May 2007 at the Hilton Bonaventure Hotel in Montreal, Quebec. WWW.CFP2007.ORG

CFP is the conference where the inventors and innovators on the Internet met the industry, the regulators, and the creative community to talk about the new freedoms the net brought. Free speech, censorship, filtering spam, crypto controls, business security, dataveillance, were all meat for the all-night debates that took place at this annual gathering.

There has never been a greater need to talk about these issues. This

year's agenda is packed with plenaries and breakout sessions,
and Birds
of a Feather sessions that look at all aspects of the growing
threats
and opportunities for autonomy in cyberspace.

Featured Speakers

- * Whitfield Diffie Sun Microsystems
- * Ron Rivest MIT
- * Simon Davies Privacy International
- * Michael Geist University of Ottawa
- * Bruce Schneier BT Counterpane
- * Kim Cameron Microsoft

* 1 full day workshop * 8 half day tutorials * Topics include: *
ID
Management * Digital Divide * Surveillance * Stalking * Wiretap
* War
on drugs * Digital Millennium Copyright Act * Charter rights *
RFIDs *
Spyware * No Fly lists * Traffic analysis * Airline Passenger
Data *
Health Information * Censorship * Data Retention * Forensics *
Security
Information Management

All this and lots more! Watch the program at www.cfp2007.org
Simultaneous Translation throughout plenary sessions
Discounts for Students and ACM Members

Stephanie Perrin, Chair CFP2007, forge@ca.inter.net

✂ CFA: joint HCMDSS and MD PNP: EXTENDED ABSTRACT DEADLINE 20 Apr 2007

<Steve Goddard <goddard@cse.unl.edu>>
Tue, 10 Apr 2007 13:19:43 -0500

Program Update and Call for Extended Abstracts
Joint Workshop On
High Confidence Medical Devices, Software, and Systems
(HCMDSS)
and Medical Device Plug-and-Play (MD PnP) Interoperability
June 25-27, 2007
Boston, MA
<http://www.cis.upenn.edu/hcmdss07>

The program for the Joint Workshop on High Confidence Medical Devices, Software, and Systems (HCMDSS) and Medical Device Plug-and-Play (MD PnP) Interoperability will feature 2-3 keynote speakers, presentations of selected technical papers, interactive panels of 3-4 speakers on important topics that require invited experts, demonstrations, and poster presentations. Papers for presentation are being selected that outline current and future directions for the development of the HCMDSS and MD PnP fields, as well as recent advances in the state of the art, with perspectives from government, industry, and academia.

A competitive Call for Papers was issued in late December and early January, and more than 30 submitted papers were received by the February 20th deadline. These were a mix of technical papers and position papers or summaries of work-in-progress. The Program Committee has reviewed these papers, and is contacting the submitters to either (1) accept the paper for a full presentation (estimated at 20 minutes plus 5 minutes for Q&A) or (2) request submission of an extended abstract (2-3 pages) on the work, which will be presented more briefly through a poster

session, as a demonstration, or as part of a panel, as decided by the workshop organizers. Submitters whose paper is accepted for a full presentation may also elect to provide a poster or a demonstration.

Extended abstracts should not exceed 3 pages (750 words). PDF format is preferred, but MS Word and PostScript are also acceptable.* The deadline for extended abstracts for all submitters is April 20th .*

Extended abstracts should be submitted by e-mail to hcmdss@cis.upenn.edu . Further information about the workshop can be found at the HCMDSS/MD PnP workshop web site, [_http://www.cis.upenn.edu/hcmdss07_](http://www.cis.upenn.edu/hcmdss07).

Julian M. Goldman, Insup Lee, Oleg Sokolsky, and Sue Whitehead
HCMDSS and MD PnP Workshop Organizers



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 64

Thursday 19 April 2007

Contents

- [BlackBerry suffers widespread outage](#)
[Monty Solomon](#)
- [Turbo Tax Servers Can't Handle E-Filing Load from Procrastinators](#)
[Cameron Wilson](#)
- [RISKS of relying on systems to file taxes late](#)
[mahlon](#)
- [US Daylight Saving Issues, System Libraries vs Program Libraries](#)
[William C Bonner](#)
- [time.windows.com failure](#)
[John Pettitt](#)
- [Philippine Internet voting system challenge](#)
[PGN](#)
- [Why should spam ever go away? The economics.](#)
[Sten Carlsen](#)
- [More on Metro software fire](#)
[Taz Daughtrey](#)
- [Re: Washington DC Metro replacing software that causes fires](#)
[Peter Rieden](#)

- [Re: On "proving NON copyright infringement"](#)
[Jim Horning](#) [Norman Gray](#)
 - [Risks of convenience](#)
[Jay R. Ashworth](#)
 - [Impossible data requested](#)
[John Harper](#)
 - [Re: Surely it can't be this easy?](#)
[Al Macintyre](#)
 - [ACM Computer Security Architecture Workshop](#)
[Jon A. Solworth](#)
 - [USENIX '07 Registration Now Available](#)
[Lionel Garth Jones](#)
 - [REVIEW: "Measuring ITIL", Randy A. Steinberg](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **BlackBerry suffers widespread outage**

<Monty Solomon <monty@roscom.com>>

Wed, 18 Apr 2007 08:10:05 -0400

The BlackBerry wireless e-mail service from Research In Motion appears to have suffered a widespread outage starting on the evening of 17 Apr (about 5:15pm PDT). The outage reportedly persisted into the following morning throughout North America. [Source: John Blau, Problem sending and receiving e-mail from BlackBerry devices appears to be limited to North America, IDG News Service, 18 Apr 2007; PGN-ed]
http://www.infoworld.com/article/07/04/18/HNblackberryoutage_1.html

✈ Turbo Tax Servers Can't Handle E-Filing Load from Procrastinators

<Cameron Wilson <wilson_c@hq.acm.org>>

Wed, 18 Apr 2007 10:24:25 -0400

Intuit (which makes TurboTax and ProSeries tax software) expected to hear from the Internal Revenue Service today (the day after taxes were due) whether any taxpayers who used its e-filing system would be penalized for submitting late returns. A flood of last-minute tax filers swamped the servers of Intuit Inc. on Tuesday, causing hours-long delays in getting forms sent in electronically to the government. As the midnight filing deadline approached, the problem got worse. During times of peak demand, Intuit was processing 50 to 60 returns per second. [Source: Lisa Leff, Associated Press, 18 Apr 2007; PGN-ed]

"Don't wait until the last minute is the moral of the story."
[Intuit spokesperson]

Last I checked, the IRS sets a legal deadline, and Intuit's FAQ on e-filing doesn't say -- maybe your filing will go through at 11:30, maybe it won't, so file early. Cameron

Cameron Wilson, Director of Public Policy, Association for Computing Machinery
1100 Seventeenth Street, NW, Suite 507 Washington DC 20036 1-202 659-9712
www.acm.org/usacm

⚡ RISKS of relying on systems to file taxes late

<mahlon <doitnow@gmail.com>>

Tue, 17 Apr 2007 23:57:27 -0700

[I include only the SECOND of two messages from Mahlon. The first gave a detailed account of repeated attempts to file electronically. PGN]

Update: At 11:54 PM, with just 6 minutes on the clock, TurboTax finally accepted my tax return. No doubt now that the East Coast is past the deadline, the load on the servers abated. (But not before I made an emergency run 40 minutes across town to the only post office open this late!)

In all, I attempted to transmit 27 separate times, receiving many nonsensical error messages. The error message that made least sense was this "no-error" error:

"No error. The transmission was unsuccessful. Please try again later."

[Link to image of the "no-error" error:

http://farm1.static.flickr.com/218/463746848_7b53305130_o.png]

Recommendations to Intuit:

1. Size your servers and network for peak volume plus contingency.
2. Provide meaningful error messages so your stressed-out users don't have to guess what's going on.
3. If the user is preparing a return during an expected high-

volume period,

provide a warning at the beginning of the process that servers may be

busy, and to file a preemptive extension while the local post office

before the local post office closes.

[Perhaps quite counter to popular opinion, but not counter-INTUIT-ively,

the IRS announced that it would accept Intuit's overly delayed returns.

(Only fitting, in that the IRS has had its own series of computer

difficulties!) An interesting RISKS question is raised, namely has the

definition of MIDNIGHT on tax-due-day been adequately specified? relative

to the time zone of the server from which the return is filed? or the

location of the filer? What if you are filing from your laptop in Hawaii

via your home or office system in NY? PGN]

⚡ US Daylight Saving Issues, System Libraries vs Program Libraries

<William C Bonner <wbonner@wimsworld.com>>

Sun, 15 Apr 2007 12:33:25 -0700

I have a Windows program written in C++ using Microsoft Foundation Class

structures. It gathers data and stores it in XML format. I store associated

time stamps for the data using ISO8601 date format, and store the dates in

UCT. (I use the ATL classes ATL::CTime for most of my time manipulation

stuff, including the FormatGmt() method.)

I do not run my own date arithmetic. I only use the library

calls for
switching between local time and UCT. I use standard library
calls for
getting the time.

In running log files from the past few weeks I've noticed that
the times
seem to be an hour off from what I remember the time would have
been when
the data was taken.

Things are more complicated, because I'm teleworking from a
location that is
two hours away from where the data was originally taken. (The
office is in
Dallas TX, I'm in Seattle WA.)

I have no idea if the various patches I've applied to the
systems I've been
using have been applied only to the operating system, the C Run
time
libraries, or only half, and making sure that they are only
applied once and
not multiple times.

I think that this US DST switch is going to continually bite us
in small
ways for several years. The only solution I see is to operate
computers on
UCT without any time zone translation enabled, which isn't
really a viable
solution.

time.windows.com failure

<John Pettitt <jpp@cloudview.com>>

Mon, 16 Apr 2007 11:05:48 -0700

time.windows.com - the system Microsoft windows machines use to set their clocks is currently reporting seemingly random times up to 150 seconds off.

It is correctly reporting stratum 16 "unsynchronized" so if the windows time

client is well written it shouldn't be a problem

🔥 Philippine Internet voting system challenge

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

Thu, 19 Apr 2007 9:57:57 PDT

Local and foreign computer hackers will be invited to break into an

Internet-based voting system that will be pilot-tested by the country's

Commission on Elections (Comelec) 10 to 30 Jul 2007 for 26,853 registered

absentee voters in Singapore. The results of the polls, which will use

survey questions, will be non-binding, which means it will not affect

official elections results.

Comelec commissioner Florentino Tuason Jr. told local reporters they have

already asked the help of the International Foundation for Electoral System

(IFES), a Washington-based IFES non-profit organization, in getting

professional hackers to test the security of the Internet voting system.

"When Scytl presented the system, everybody was impressed on the security

features. It is covered by international patent and it has been declared

secured by no less than Switzerland and everyone in the global community

should respect that decision," Tuason told reporters in a conference Tuesday. Scytl's computerized voting system is also being used in countries such as the U.S., Switzerland, and Belgium.

The Comelec has earlier batted for the full implementation of the Internet voting system in Singapore but Senator Richard Gordon succeeded in stopping it. Gordon wanted a computerized casting and counting system to be deployed instead in selected provinces in the country. The Comelec had to back off, however, because it lacked enough time to prepare for this type of system.

[Source: Geoffrey Ramos, Hackers Invited To Break Into Philippine Internet Voting System, *All Headline News*, Manila, Philippines (AHN), 17 Apr 2007;

thanks to Paul Lambert for spotting this one]

<http://www.allheadlinenews.com/articles/7007075062>

Why should spam ever go away? The economics.

<Sten Carlsen <stenc@s-carlsen.dk>>

Wed, 18 Apr 2007 22:51:48 +0200

So, why would spam go away?

The economics of spam will eventually decide whether spam will go away or not. If somebody can make money from it, it will stay.

I tried to grasp the total picture of the economics of spam in the following text. I am sure I missed something.

Who gains at the present situation:

- * spammers get paid by crooks and businesses
- * backbone providers get to sell more bandwidth
- * BOTnet providers get paid for their BOTnets
- * ISPs can sell extended security packages and filtering services
- * Spam-filter companies make their living off the spam
- * politicians can get new laws accepted that will give them more control
- * virus writers get paid for writing BOTnet creating viruses and trojans

Who loses at the present situation:

- * users have to pay more for their connections
- * ISPs have to pay more for their backbone
- * software companies have to use substantial resources to make security updates
- * companies, whose employees waste time to sort through loads of spam before work can be done

IF spam should go away, who gains:

- * users should get cheaper prices
- * ISPs would have cheaper backbones because of less traffic
- * software companies would have less incentive to make safe software
- * companies, whose employees no longer waste time to sort through loads of spam before work can be done

IF spam should go away, who loses:

- * back bone providers will lose about half their market
- * BOTnet providers will lose most of their market, leaving only virus and attack parts
- * virus writers would lose their main source of income
- * ISPs would lose the market for filtering services
- * spam-filter companies would lose their whole market
- * spammers would lose their income

- * politicians would have less excuse for controlling the Internet
- * some businesses would have to find more expensive advertising channels

So, why do you think spam would ever go away. Who would want it to go away?

Sten Carlsen

✦ More on Metro software fire (Epstein, [RISKS-24.63](#))

<"Daughtrey, H. Taz" <DAUGHTHT@CS.JMU.EDU>>

Mon, 16 Apr 2007 18:47:35 -0400

I have yet to discover the exact nature of the software "designed to monitor the flow of electricity" and would appreciate any more details.

Follow-up coverage indicated the problem software was in the newest model (6000-series) cars, as well as older (2000- and 3000 series) cars that Alstom was contracted to refurbish. Metro operates a total of 190 cars with the monitoring software package that malfunctioned. Officials had replaced the software with an older version in about 150 cars by Friday, April 13. The previous version of software was to be reinstalled in about 40 additional rail cars during offpeak hours Friday night and Saturday morning. Reverting to the old software takes about 20 minutes for each rail car, and all fixes were to be paid for by Alstom.

<http://washingtontimes.com/metro/20070412-104206-9871r.htm>

An extensive December 2006 audit report by the Washington

Metropolitan Area

Transit Authority identified deficiencies in Alstom's software quality processes, but none seem to relate specifically to this problem.
http://www.wmata.com/about/parp_docs/Internal_Audit_Rail_Car_Report_010307.pdf

✶ Re: Washington DC Metro replacing software that causes fires

<"Rieden, Peter \(\UK\) " <Peter.Rieden@baesystems.com>>

Mon, 16 Apr 2007 17:07:51 +0100

The "Software causing hardware problems" phenomenon can be a troubling one. It has been a fundamental tenet of modern systems engineering that the advantage of software-based systems over hard-wired ones is that additional functionality can be added at much lower cost, especially in the basic qualification of the hardware elements. For example consider a mission computer in a modern military fast jet. This would be initially integrated onto the aeroplane and in the process it would be tested for all the usual things - shock, bump, thermal environment, EMC etc etc. Some time later it is decided to integrate a new type of sensor array into the starboard tachyon emitter, and this requires a small amount of additional code in the mission computer to enable the sensor to be controlled from the existing pilot controls and to direct the sensor output to the cockpit displays (and over the sub-ether JTIDS net back to Starfleet HQ).

Now obviously the upgraded mission computer software would have to go through the normal integration test/qualification process - everyone can see that. And equally obviously the physical clearances on the mission computer *hardware* could just be read across, because we haven't changed anything, have we? After all, we only changed the software. Well unfortunately this isn't true. Firstly this sensor presents primarily hi-resolution, rapidly changing video images, so the video processor in the MC is now running at five times the utilisation that it was with the previous software, and thus runs hotter. This influences the thermal environment inside the MC and knocks onto the cooling requirements of other internal subsystems so that now the numeric processor overheats and fails after 10 minutes. There are some people who spot this one, so whilst it's rare it's not unheard of to consider whether the thermal qualification of the equipment should be revisited as part of the design process.

But what about the EMC qualification? We've changed nothing *outside* the box and the new sensor is only communicating over the existing Mil-Std-1553 databus, so this [expensive] testing surely doesn't need repeating. Or does it? The MC was designed with upgrade capacity in all major respects, and one of these is I/O - there are a number of unused interfaces or a variety of types in the I/O subsystem. But that's not a problem because they're all clamped low in the software. So when an unintended coding error inadvertently unclamps one of the inputs (a high impedance one) and admits

external signals the condition is not checked in testing. This signal is then picked up by an adjacent small-signal navigation input which IS used, and corrupts its data - something that isn't discovered until the system enters service and is illuminated by Klingon sensor beams.

Of course this is a purely hypothetical case, and has certainly never happened on any major military fast jet programme in the western world. Not ever. No sir, absolutely not! The very idea! But it is perhaps worth remembering that software changes the characteristics of hardware, so when designing ANY software change the qualification of the hardware (and the required test cases) should ALWAYS at least be formally reviewed and repeated where necessary.

PDR

✉ Re: On "proving NON copyright infringement" (Reinke, [RISKS-24.63](#))

<"Horning, Jim" <Jim.Horning@sparta.com>>

Mon, 16 Apr 2007 12:16:22 -0700

The idea of a digital notary was patented some time ago, and a company (Surety Technologies, Inc.) started to provide the service. But it was not a great commercial success.

<http://www.interesting-people.org/archives/interesting-people/199403/msg00100.html>

http://www.math.columbia.edu/~bayer/papers/Timestamp_BHS93.pdf
<http://www.sciencenews.org/pages/pdfs/data/1995/147-09/14709-15.pdf>
<http://www.oasis-open.org/committees/dss/ipr.php>

[Also noted by Jeremy Epstein. PGN]

Re: On "proving NON copyright infringement" (Re: Reinke, R-24.63)

<Norman Gray <norman@astro.gla.ac.uk>>

Wed, 18 Apr 2007 11:45:50 +0100

Ferdinand Reinke suggests a digital notary service, and describes a number of cases, and a number of keypairs. There might be a simpler orp protocol.

1. I want to notarise my wonderful protocol document, before showing it to the venture capitalists. So I send an SHA1 sum of it to the notary.
2. The notary publishes it on a webpage (or a newsgroup or a mailing list), along with the list of all the similar sums they've seen today, or this week, or this month. They let the Internet back it up; I'll certainly hold on to a copy.
3. At the same interval as the notary publishes that list, they publish its checksum in some suitable newspaper of record.

In fact, you could do step 3 yourself, and short-circuit the whole process,

but where's the VC fun in that?

In fact, something like this has been running since 1995, at <http://www.itconsult.co.uk/stamper/stampinf.htm>. It's concerned with the slightly more elaborate problem of corroborating when a document was PGP signed, and publishes its summaries to comp.security.pgp.announce (the only thing there apart from spam, as far as I can see).

I fear a single chequebook may continue to be sufficient...

All the best,

Norman Gray : <http://nxg.me.uk> eurovotech.org : University of Leicester, UK

✶ Risks of convenience

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

Tue, 17 Apr 2007 15:23:58 -0400

It is said that 'security is inversely proportional to convenience', and a recent contribution to RISKS illustrates this proposition quite well.

In 24.63, David Brunberg, writing on the British crushed car fiasco, says:

> As has been reported elsewhere,

> <http://www.cs.cmu.edu/afs/cs.cmu.edu/user/wbardwel/public/nfalist/rip/index.html>

> the NFRTR has been in deplorable condition for some time.

> Many registration documents have been lost by ATFE, and some were even

> willfully destroyed by ATFE contract employees in a well documented

> case.

My apologies for the wrapped URL... but lets take a closer look
at that
URL, shall we? Oh, my: it seems to be an Andrew File System
path, exposed
via the campus's CS department webserver.

Convenient? Certainly.

But making the individual components of a) CMU's internal DNS
and b) the
pathnames of files on individual machines in that domain visible
to the
general public at large is a decision that, perhaps, could use
some
additional review?

We know now not only that user's internal id, but also the name
of his
machine, and several details of his internal directory
structure, which
might leak useful information to the outside world.

In this *particular* case, of course, the machine is the central
CS machine,
and the file in a user's public subdirectory. But students or
staff at that
university might well be able to take advantage of their
knowledge of
internal conventions on such issues...

There's a second possible layer of the same problem in the fact
that AFS
uses DNS for it's second address layer, if in fact that's wired
into the
protocol -- I'm not that familiar with AFS.

But all these versions of this problem imply a certain
requirement for
administrative and architectural care -- designing a network
where these
requirements won't leak information useful to a Bad Guy, if

possible -- and possibly also user training -- if you can't tighten things all the way, then your users will have to exercise due care.

Similar examples exists where @aol.com e-mail addresses are generally usable for attempting to contact someone via AIM, and where SMS addresses are generally the same as the voice number for a cellphone; these are both instances where some circumstances would make it useful for those namespaces to be disjoint...

Certainly readers can discern other similar namespace overloading situations for themselves, and intuit the potential problems...

Jay R. Ashworth, Ashworth & Associates, St Petersburg FL USA
+1 727 647 1274 <http://baylink.pitas.com> jra@baylink.com

✶ Impossible data requested (... Citizenship No., CJB, [RISKS-24.63](#))

<John Harper <John.Harper@mcs.vuw.ac.nz>>
Mon, 16 Apr 2007 11:52:03 +1200 (NZST)

This sort of thing happens in North as well as South America. One reason I closed my US bank account was that I couldn't use its web site because it insisted on being told my 5-digit zip code. New Zealand and Australia use 4 digits, and UK uses varying numbers of letters and digits, and also a blank space in the middle. The obvious conclusion was that the bank didn't want its non-US customers. (The bank wasn't the same one I had opened

an account
at in Evanston, IL, when living there for a few months, but was
the one that
took over the one that took that one over.)

New Zealand's provinces were abolished in November 1876, but
many North
American web sites ask for my state or province. I know which
one Wellington
was in, and I duly tell the inquirers, but what do they do with
data 130
years out of date?

John Harper, Statistics and Computer Science, Victoria
University,
PO Box 600, Wellington 6140, New Zealand (+64)(4)463 5341

✉ **Re: Surely it can't be this easy? (Lee, [RISKS-24.63](#))**

<Al Macintyre <macwheel99@sigeom.net>>
Sun, 15 Apr 2007 13:58:58 -0500

I was staying at a major hotel chain, returned to my room to
find that the
key card would not work. I was retrying it, jiggling door etc.
when another
guest came to the door. He had just checked in, my stuff was
still in the
room from me getting there earlier. We went to front desk
together to get
this straightened out.

Turns out, the hotel key card system is on a different computer
than the
hotel reservations and guest billing system. They check us in,
write down
our # on the little envelope the key card goes in, then in the
door security

system, rescrumble that door password & the computer writes it onto the magnetic strip given to latest guest. When transcribing guest room # from billing computer to envelope, or into the door security system, in the words of the desk clerk "Mistakes happen ALL THE TIME."

In our case, they had intended to give the new guest some other room than the one for me. There are other combinations of what can go wrong with the system. So when you get into your room, be sure to lock yourself in ... you could be taking a shower, in bed, along comes another guest.

In wee hours, the front desk not attended, you have to ring the bell a lot. Seems to me the computer systems accessible to some crook who would not ring the bell.

When I got back home, I told co-workers about this. It had been on a business trip. Co-workers who travel more often than me told me that this sort of thing is not unusual.

ACM Computer Security Architecture Workshop

<"Jon A. Solworth" <solworth@rites.uic.edu>>
Wed, 18 Apr 2007 23:15:54 -0500

The First ACM Computer Security Architecture Workshop (CSAW, pronounced SEE-SAW) will be held 2 Nov 2007 at George Mason University in Fairfax, Virginia, in conjunction with the 2007 ACM Conference on Computers and

Communications. Papers on system security architectures, their interfaces, implementations, and implications are due by 17 Jun 2007. See the website for details:

<http://www.rites.uic.edu/csaw>

USENIX '07 Registration Now Available

<Lionel Garth Jones <lgj@usenix.org>>

Fri, 13 Apr 2007 15:36:00 -0700

2007 USENIX Annual Technical Conference
June 17-22, 2006, Santa Clara, CA
Early Bird Registration Deadline: June 1, 2007
<http://www.usenix.org/usenix07/proga>

Jeff Chase, Duke University
Srinivasan Seshan, Carnegie Mellon University
USENIX '07 Program Co-Chairs
usenix07chairs@usenix.org

REVIEW: "Measuring ITIL", Randy A. Steinberg

<Rob Slade <rmslade@shaw.ca>>

Tue, 17 Apr 2007 13:12:15 -0800

BKMSITIL.RVW 20070119

"Measuring ITIL", Randy A. Steinberg, 2006, 1-4120-9392-9

%A Randy A. Steinberg RandyASteinberg@aol.com

%C Suite 6E, 2333 Government Street, Victoria, BC V8T 4P4

%D 2006

%G 1-4120-9392-9

%I Trafford Publishing
%O 888-232-4444 FAX 250-383-6804 sales@trafford.Com
%O [http://www.amazon.com/exec/obidos/ASIN/1412093929/
robladesinterne](http://www.amazon.com/exec/obidos/ASIN/1412093929/robladesinterne)
[http://www.amazon.co.uk/exec/obidos/ASIN/1412093929/
robladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/1412093929/robladesinte-21)
%O [http://www.amazon.ca/exec/obidos/ASIN/1412093929/
robladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/1412093929/robladesin03-20)
%O Audience s- Tech 1 Writing 1 (see revfaq.htm for
explanation)
%P 154 p.
%T "Measuring ITIL"

Chapter one is supposed to be an introduction to the book. Unfortunately, it jumps right in without bothering to define some basics (such as what ITSM is, and why we should want to measure it). (It probably stands for Information Technology Services Management, since ITIL, the Information Technology Infrastructure Library is about that topic.) Purportedly an overview of metrics, chapter two is actually an exhortation to measure things. Aspects of a metrics model framework are listed in chapter three, although the details don't do much to explain any overall structure or operation.

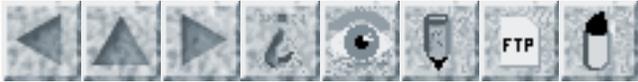
Chapter four is a set of tables of incident response metrics. Unfortunately, the material is cyclically self-referential, without ever explaining real details. Similar non-definitions are given for various management areas in subsequent chapters: problems in five, change in six, release in seven, configuration in eight, service desk (no management) in nine, service levels in ten, availability in eleven, capacity in twelve,

service continuity in thirteen, IT financials in fourteen, and IT workforce in fifteen. (If you are well familiar with ITIL you will recognize the structure, but the book does not explain it.)

Chapter sixteen suggests that if you have very few sources of metrics, then you should collect and display a few metrics. Chapter seventeen describes the DICE (Duration, Integrity, Commitment, Effort) model that attempts to predict the likelihood of success of an ITIL (the first time the Information Technology Infrastructure Library is materially mentioned in the book, despite the title) implementation. Unfortunately, the text stops short of really explaining how to use the model, or calculate the parameters you are to enter. There is a tiny bit more information on the ITSM Metrics Model Tool, in chapter eighteen, but unfortunately the detail is on the output side, rather than input. Chapter nineteen outlines a full program (including an enormous staff) for using the metrics, but, since everything is based on measurements that have not been fully explained, it is hard to say how useful all of this is.

If you are fully versed in ITIL, this book might help you decide how to measure your operations. Mind you, if you are completely familiar with ITIL, and are using it, you probably already have your own metrics in hand.

copyright Robert M. Slade, 2007 BKMSITIL.RVW 20070119
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<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

Search RISKS using [swish-e](#)

Volume 24: Issue 65

Tuesday 24 April 2007

Contents

- [A new book on risks by Charles Perrow, The Next Catastrophe](#)
[PGN](#)
- [Gov't Straining to Secure Computer Systems](#)
[PGN](#)
- [Don't let your navigation system fool you](#)
[PGN](#)
- [KPMG profile of a fraudster](#)
[Rob Slade](#)
- [US Dept of Agriculture & Census Bureau have long contained SSNs](#)
[Kenneth C Knowlton](#)
- [Automatic translation leads to ethnic slur](#)
[Jeremy Epstein](#)
- [Prisoner freed by fax](#)
[Bob Morrell](#)
- ["System problems" on a departing airline flight?](#)
[A.E. Siegman](#)
- [Elections bring down foreign Web sites](#)
[Bertrand Meyer](#)

- [Netcraft Data for Ohio Secretary of State Web site](#)
[McGrude](#)
 - [Audit Finds Many Faults in Cleveland's 2006 Voting](#)
[David Lesher](#)
 - [Re: Philippine Internet voting system challenge](#)
[David Lesher](#)
 - [Re: Washington DC Metro replacing software that causes fires](#)
[Barry Gold](#)
 - [RIM cites upgrade glitch for BlackBerry outage](#)
[Robert Israel](#)
 - [Re: US Daylight Saving Issues](#)
[Larry Jones](#) [Charlie Shub](#)
 - [Re: Risks of relying on systems to file taxes late](#)
[Rex Black](#) [Ross Oliver](#)
 - [REVIEW: "Information Security Awareness Basics", Fred Cohen](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ A new book on risks by Charles Perrow, *The Next Catastrophe*

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

Tue, 24 Apr 2007 12:05:47 PDT

Charles Perrow,
The Next Catastrophe:
Reducing Our Vulnerabilities to
Natural, Industrial, and Terrorist Disasters
Princeton University Press, 2007, viii+377

Charles Perrow's earlier book, *Normal Accidents: Living with High-Risk Technologies* (Basic Books, New York, 1984), was an enormously important inspiration for many early RISKS readers. His latest book is likely to be even more important, and certainly very timely. From the

jacket: This book is "a penetrating reassessment of the very real dangers we face today and what we must do to confront them."

On a personal note, when I called him out of the blue in the late 1980s and asked him if he would keynote one of the COMPASS conferences (predecessors to the ACM ACSAC conferences), he demurred -- saying he was not a computer expert. And yet his message was completely on the mark for that audience and for RISKS back then. Twenty years later, there is no question that his writing is absolutely relevant to the huge set of technological and social problems we face today. The message of his new book is very clear: we must do much more to reduce the vulnerabilities across the board. "Rather than laying exclusive emphasis on protecting targets, we should reduce their size to minimize damage and diminish their attractiveness to terrorists." His analyses of FEMA, DHS, 9/11, and Katrina are incisive. He makes a very strong case for the need to make major changes in what has seemingly become a rather business-as-usual response to past catastrophes and a pervasive unwillingness to adequately anticipate future catastrophes. I consider this book essential reading for all RISKS readers.

The book very clearly addresses the computer-related risks as well as many others. The holistic view of the book is absolutely essential if we are going to confront the next catastrophe(s). I recommend it highly. PGN

[I note an ambiguity in the subtitle that most of you will

probably miss.

In addition to the intended emphasis on Reducing Our Vulnerabilities,

there is an unintended secondary interpretation (as in "Reducing a complex

problem to a simpler problem"), suggesting that if (for example) we could

get rid of all of the computer-related risks that result from flawed

designs, buggy implementations, human errors in operations, and so on (and

which are so prevalent in RISKS), we could reduce our vulnerabilities to

only a much smaller subset, namely, just natural, industrial, and

terrorist disasters -- and nothing else. This may seem obscure to

nonEnglish speakers, and is clearly not what is meant by the title, and

thus I include it here as a squarely parenthetical aside.]

🔥 Gov't Straining to Secure Computer Systems

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

Tue, 24 Apr 2007 10:22:13 PDT

Federal computer networks are being targeted on an unprecedented scale and

recent high-profile compromises at the Departments of Commerce and State are

likely just the most visible symptoms of a government-wide security

epidemic, government security experts told a House Homeland Security

Committee hearing. [Source: Hackers Increasingly Gaining Access to

Networks, Congress Is Told, Brian Krebs, *The Washington Post*, 19 Apr 2007]

⚡ Don't let your navigation system fool you

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

Tue, 24 Apr 2007 10:22:28 PDT

Two Italian hackers have figured out how to send fake traffic information to navigation systems that use a data feature of FM radio for real-time traffic information. Using cheap, off-the-shelf hardware, they can broadcast traffic data that will be picked up by cars in about a one-mile radius, the hackers said during a presentation at the CanSecWest event here.

"We can create queues, bad weather, full car parks, overcrowded service areas, accidents, roadwork and so on," Andrea Barisani, chief security engineer at Inverse Path, a security company. "Traffic information displayed on satellite navigation systems is trusted by drivers. Normal people do not think that you can do nasty things."

Barisani and hardware hacker Daniele Bianco discovered that the system used by many navigation aides to get traffic data isn't secured. The data is sent using the Traffic Message Channel (TMC) of the Radio Data System (RDS), a standard way of transmitting data over FM radio also used to display station names and program titles. [Source: Joris Evers, CNET News.com, 20 Apr 2007: PGN-ed]

KPMG profile of a fraudster

<Rob Slade <rMslade@shaw.ca>>

Thu, 19 Apr 2007 11:56:50 -0800

KPMG UK has produced a report to help us identify people who would defraud our companies. It is interesting, mostly in terms of the questionable nature of the conclusions.

[http://www.kpmg.co.uk/pubs/ProfileofaFraudsterSurvey\(web\).pdf](http://www.kpmg.co.uk/pubs/ProfileofaFraudsterSurvey(web).pdf)

The profile is based on 360 cases of detected and investigated fraud, in Europe, South Africa, and the Middle East.

The 38 page report is initially long on platitudes, although it does provide data in the later stages. The "personal" profile (on page 8) is probably the most interesting part:

70% of fraudsters were between the ages of 36 and 55 years old, and so in the later stages of their career.

85% male.

68% acted independently.

89% insiders. (We knew that ...)

60% senior management. An additional 26 % of frauds involve management level persons bringing the total to 86 % of profiles involving management.

87% employed 2 years or more at the company defrauded. (Highest proportion

in the 3-5 year range.)

The internal fraudster most often works in the finance department followed by operations/sales or as the CEO.

The response suggested by the report is vague. The recommendations are the same that we've all heard, with a heavy emphasis on "internal controls."

However, the data in the profile doesn't necessarily support this advice:

internal controls are not terribly effective, according to the reports.

confession of perpetrator 2%
negligence of perpetrator 2%
complaints by suppliers 4%
accidentally 8%
complaints by customers 9%
suspicious superior 9%
internal controls 10%
external controls 10%
management review 21%
whistle blowing 25%

(The type of fraud is also interesting:

counterfeit 1%
insider trading 1%
money laundering 2%
breach of secrets 2 %
other fraud 9%
embezzlement 10%
theft of other assets 10%
false financial reporting 20%
theft of cash 22%
corruption 23%

This is the data from Europe. Theft of cash and "corruption" are higher in South Africa and the Middle East figures.)

rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>

✦ US Dept of Agriculture & Census Bureau have long contained SSNs

<Kenneth C Knowlton <KCKnowlton@aol.com>>

Sun, 22 Apr 2007 09:46:23 EDT

The U.S. Department of Agriculture has for many years publicly been listing Social Security numbers of about 30,000 people who received financial aid from two of its agencies, raising concerns about identity theft and other privacy violations, apparently unbeknownst to DoA and Census Bureau officials -- until an Illinois farmer stumbled onto the data via Google at FedSpending.org. [Source: U.S. Database Exposed Social Security Numbers, Ron Nixon, *The New York Times*, 21 Apr 2007; PGN-ed]
<http://www.nytimes.com/2007/04/21/washington/21data.html?th&emc=th>

✦ Automatic translation leads to ethnic slur

<Jeremy Epstein <jepstein@webmethods.com>>

Fri, 20 Apr 2007 10:24:33 -0400

The automated translation of a color description by a Chinese manufacturer

into English resulted in an ethnic slur (which I'm not repeating here due both to its being offensive and to avoid tripping inappropriate word filters). While there are periodic lists circulated around of mistranslations, this one wasn't funny but rather quite offensive. There's the usual level of finger-pointing between the retailer, wholesaler, and manufacturer of who is responsible.

Some lessons learned:

- Translations should be checked by a native speaker to ensure both accuracy and appropriateness.
- Relying on automated translations as a cost saving measure isn't a good idea, for anything other than getting the gist of an idea.

<http://www.cnn.com/2007/WORLD/americas/04/19/canada.couch.ap/index.html>

[Also noted by several others. PGN]

✶ Prisoner freed by fax

<"Bob Morrell/Cancer Center" <bmorrell@wfubmc.edu>>

Mon, 23 Apr 2007 12:13:38 -0400

A prisoner was wrongly released after a fax was received from a grocery store stating that the Kentucky Supreme Court had demanded his release:

<http://www.cnn.com/2007/US/04/21/wrongly.freed.ap/index.html>

I have always complained that network security is held to a standard that other technologies do not have to meet. Apparently others

are
noticing this as well...

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

Sun, 22 Apr 2007 12:07:30 -0700

While waiting to board a different flight in the United Terminal at JFK Friday evening, April 20, I was bemused to hear an announcement repeated perhaps 20 times in a two-hour period:

"Attention passengers on British Airways flight 1502 to Manchester: Due to system problems on this aircraft, there will be no inflight entertainment and no overhead lighting during the flight. We apologize for this inconvenience; passengers who have questions may come to Gate xxx."

I guess my own question would have been: Do I want to head out over the Atlantic in an aircraft that's having "system problems" and especially electrical ones? (Maybe it would depend on whether I'd gotten an upgrade or not . . .)

A. E. Siegman, McMurtry Professor of Engineering Emeritus,
Stanford University
(650) 326-4360 siegman@stanford.edu

[This seems to be a not uncommon failure mode, which I presume the repair folks believe is unrelated to the flight controls. On the other hand,

RISKS readers are generally suspicious of such beliefs. I suppose that if this particular problem cannot be fixed quickly enough, the airline might prefer not to delay the flight, which of course can have propagational effects on international schedules. PGN]

✈ Elections bring down foreign Web sites

<Bertrand Meyer <Bertrand.Meyer@inf.ethz.ch>>

Sun, 22 Apr 2007 21:05:15 +0200

The current French presidential election provides rich material for RISKS, in particular many stories related to the somewhat botched introduction of voting machines. Here is a report on the Web consequences, as seen by one "Internaute", of today's (22 April 2007) first round of balloting.

French law prohibits any publication of estimates in the last two days and until the closing of the polls at 8 PM; in recent years it was extended to cover the Internet. Partly because penalties for breaking the ban are serious, and partly because the rule enjoys broad support, no reputable French Web site was tempted to publish any estimate before the deadline (although lemonde.fr reported at 18:46 that the mood at one of the principal candidate's headquarters was "not ebullient", a rather blatant giveaway). Neither was it easy to find a list of links to the sites of foreign news media, to which the rule cannot apply.

Several of these foreign sites, especially those of French-language papers in Belgium and Switzerland, had announced that they would start giving out estimates at 6 PM, when exit polls provide a credible picture. *La Libre Belgique*, for example, explicitly invited Web readers to come at 6.

Starting in the afternoon, most of these sites (*La Libre Belgique*, *Le Soir* from Brussels, *Le Matin* from Lausanne...) were, for me at least, impossible to reach; they were timing out. It looked like all of wired France (Internet penetration per Nielsen: 50.3% in late 2006) was trying to access them, and either the servers or the bandwidth couldn't follow. Long into the evening I still couldn't reach lalibre.be.

I got my first taste of the results around 6:30 through an Italian site, *Corriere della Sera*; other Italian newspapers such as *La Repubblica* had estimates shortly thereafter. One of these reports pointed to Swiss French-speaking TV (I hadn't checked tsr.ch earlier but it was working properly when I did). The Swiss German-language newspaper sites (NZZ, *Tagesanzeiger*) published the estimates a few minutes later. In stark contrast with foreign French-language sites, none of the non-French-language sites showed any sign of stress.

At some point in the afternoon someone at *Le Temps* (Geneva), whose site had been slow but reachable, had the good sense to replace the site's usual home page -- with the usual combination of ads, photographs, cartoons,

links, tables, CSS and other complicated layout -- by a text-only page entirely devoted to a concise report about the French election, with a note that traffic was unusually high and that the normal page would be restored later. As a result one could find estimates there too. Le Soir eventually did the same.

If this experience is representative, it would seem that the infrastructure for many newspapers' online editions isn't ready to withstand a steep surge in visits. True, today's situation was exceptional because of the news blackout about an event that has generated considerable passion (the turnout was the highest ever, and the outcome was hard to predict) in a large country whose language is spoken by much smaller neighboring communities. Scaling up a site to accommodate millions of foreign visitors on a couple of afternoons every few years probably doesn't sound like an attractive investment; it is unlikely to yield many new advertisers or subscribers. Still, one can wonder about the effect on these sites of the next major news event.

It is surprising to see how few sites had *Le Temps*'s reaction of providing a pared-down, text-only version of the site with the key information that visitors are seeking. Granted, such sites are there to sell advertisements, not provide a public service; but a site that no one can access doesn't do much for advertisers or anyone else. It seems that other media sites didn't have any contingency planning, or didn't even realize what was going on.

The second round, of only two candidates, is two weeks from now, with the same law in force and presumably even higher stress and eagerness to know. It's going to be interesting to see if the sites are better prepared this time.

One site, cnn.com, was as usual available all the time without any delay; until shortly before 8 all that one could find on the home page was a link to older material about the campaign. The text of the link was expressing a world philosophy more eloquently than many a long speech: "French polls open; candidates differ on U.S.".

Bertrand Meyer ETH Zurich <http://se.ethz.ch> Eiffel <http://www.eiffel.com>

Netcraft Data for Ohio Secretary of State Web site

<McGrude <McGrude@gmail.com>>

Tue, 24 Apr 2007 13:15:10 -0700

"Netcraft is showing that an event happened in the Ohio 2004 election that is difficult to explain. The Secretary of State's website, which handles election reporting, normally is directed to an Ohio-based IP address hosted by the Ohio Supercomputer Center. On Nov. 3 2004, Netcraft shows the website pointing out of state to a server owned by Smartech Corp. According to the American Registry on Internet Numbers, Smartech's block of IP

addresses

64.203.96.0 - 64.203.111.255 encompasses the entire range of addresses owned

by the Republican National Committee. Smartech hosted the recently notorious

gbw43.com domain used from the White House in apparent violation of the

Presidential Records Act, from which thousands of White House e-mails

vanished. Can anyone suggest a good explanation for this seemingly dubious

election-eve transfer?"

<http://www.alternet.org/story/50941>

<http://politics.slashdot.org/politics/07/04/24/1735213.shtml>

http://toolbar.netcraft.com/site_report?url=http://election.sos.state.oh.us

✶ Audit Finds Many Faults in Cleveland's 2006 Voting

<David Leshar <wb8foz@panix.com>>

Thu, 19 Apr 2007 23:35:02 -0400 (EDT)

An audit of the November 2006 general election in the Cleveland area has

found that hundreds of votes were lost, others were recorded twice, and

software used to count the ballots was vulnerable to data problems.

[Source: Bob Driehaus, *The New York Times*, 20 Apr 2007; PGN-ed]

✶ Re: Philippine Internet voting system challenge ([RISKS-24.64](#))

<David Leshar <wb8foz@panix.com>>

Thu, 19 Apr 2007 20:42:21 -0400 (EDT)

[David's note refers to the major inherent problem with Internet voting, coercion/vote selling. PGN]

- a) Go to voter's house ahead of time.
- b) "See my gun? You will vote as I tell you, while I watch; or I'll take your daughter with me... and sell her, if she's still alive."
- c) Voter decides that Gov. Dewey is not a bad choice after all.

Repeat as needed.

I can't recall who coined the phrase "rubber-hose cryptanalysis" but it also applies to voting. There IS a reason we have the secret ballot.

The RISK? Worrying about only one RISK, and ignoring the others...

Re: Washington DC Metro replacing software that causes fires

<Barry Gold <barrygold@ca.rr.com>>

Thu, 19 Apr 2007 22:28:17 -0700

(Rieden, [RISKS-24.64](#))

- > ... when designing ANY software change, the qualification of the hardware
- > (and the required test cases) should ALWAYS at least be formally reviewed
- > and repeated where necessary.

Well, the NSA is well aware of this, and I'm a little surprised that the people who design aircraft -- especially military aircraft --

aren't. If you look at DCID 6/3 and supporting material you will see a pretty good set of specifications.

This applies especially to systems designed for Protection Level 7 -- systems that will handle data spanning from unclassified/general public to Top Secret with one or more Special Access Need-to-Know Compartments. Such systems would need to be built to EAL-7 (formerly called A-1 in the old Orange Book). This requires a full mathematical specification of the software, mathematical proof that the specification preserves security, and a line-by-line correspondence between the specification and the code.

In practice, this takes a lot of time. Just building a system of any size takes time, and then you need to add effort and time to write and prove the formal specification and the code correspondence. And then the whole thing has to be reviewed by a certifying authority.

So the usual result is that you have built an EAL-7 boat anchor. By the time you've done all this, your system is two years out of date -- too old to be useful in today's rapidly evolving world. The best you can do is keep the same software and match it with newer, more modern hardware. But then the new hardware has to go through the certification process too.

The only commercial product I'm aware of that meets EAL-7 is the Data Diode -- magnificent in its simplicity. It keeps data from flowing the "wrong" way (from more classified to less classified) by the simple

technique of not providing a hardware path for that data flow. At its heart is a fiber-optic cable, one end has (only) transmitters, and the other end has (only) receivers. There is simply no way to move data the other way.

✦ RIM cites upgrade glitch for BlackBerry outage ([RISKS-24.64](#))

<Robert Israel <israel@math.ubc.ca>>
Sun, 22 Apr 2007 10:17:36 -0700 (PDT)

<http://www.globeinvestor.com/servlet/story/GAM.20070421.RRIM21/GIStory/>

A few excerpts:

RIM co-chief executive Jim Balsillie dismissed those worries, telling Reuters News Agency that "systems are in place so that this kind of thing, as incredibly unlikely as it is to happen, is all the more unlikely to happen again." [where have we heard that one before?]

Essentially, he said, "it was an outage overnight when there was an upgrade."

But the outage has also raised concerns about the way RIM handles e-mail data, Mr. Levy said, given that all traffic is routed through a single communication centre.

Robert Israel, Department of Mathematics, University of British Columbia
Vancouver, BC, Canada <http://www.math.ubc.ca/~israel>

Re: US Daylight Saving Issues (Bonner, [RISKS-24.64](#))

<Larry Jones <lawrence.jones@ugs.com>>

Fri, 20 Apr 2007 21:30:36 -0400 (EDT)

> In running log files from the past few weeks I've noticed that
> the times
> seem to be an hour off from what I remember the time would
> have been when
> the data was taken.

When converting between local time and UTC, Microsoft has long held the peculiar philosophy that whether Daylight Saving Time is **currently** in effect should be used to determine the offset to be applied rather than whether DST was (or will be) in effect at the time being converted. This has caused no end of problems, but they insist that that is how it's supposed to work and refuse to fix it.

Re: US Daylight Saving Issues (Bonner, [RISKS-24.64](#))

<Charlie Shub <cdash@ludell.uccs.edu>>

Thu, 19 Apr 2007 22:19:28 -0600 (MDT)

The solution seems rather obvious. Instead of using software to account for all the idiosyncracies in time calculation, the process should be data driven, through a configuration file. When will we ever learn?

Charlie Shub, University of Colorado at Colorado Springs (719)
262-3492

<http://cs.uccs.edu/~cdash> cdash@cs.uccs.edu

⚡ Re: Risks of relying on systems to file taxes late ([RISKS-24.64](#))

<Rex Black <rexblack@ix.netcom.com>>

Thu, 19 Apr 2007 19:43:30 -0500

> "Don't wait until the last minute is the moral of the story."

Actually, the moral of the story is:

1. Save money by not bothering to load test your software.
2. Blame your customers for the performance and reliability bugs you didn't find and shift the costs off to them should any costs occur.
3. Convince--somehow or other--the Federal government that you shouldn't be fined or at least stripped of your privilege to process taxes online.

Since they seem to have pulled off this little trifecta, the title of this story is: "Software Quality Doesn't Matter: Part 11,765 in a Continuing Series."

Rex Black, President, American Software Testing Qualif. Board;
Pure Testing,
31520 Beck Road, Bulverde, TX 78163 1-830-438-4830 www.rexblackconsulting.com

⚡ Re: Risks of relying on systems to file taxes late

<Ross Oliver <ross599@yahoo.com>>

Fri, 20 Apr 2007 15:41:47 -0700 (PDT)

I am not a tax professional, but I think it is worth pointing out that the April 15th (17th this year) date is the deadline to pay any income tax owed without penalty. If the government owes you a refund, there is no penalty for filing a return after this date. The IRS is more than happy to remain caretaker of your money. I believe a widespread misunderstanding of the deadline was contributing factor to the filing frenzy and resulting online meltdown. Perhaps Intuit should add this information to its "try again later" messages.

REVIEW: "Information Security Awareness Basics", Fred Coheno

<Rob Slade <rMslade@shaw.ca>>

Fri, 20 Apr 2007 12:35:58 -0800

BKINSCAB.RVW 20070119

"Information Security Awareness Basics", Fred Cohen, 2006,
1-878109-39-1

%A Fred Cohen

%C 572 Leona Dr, Livermore, CA 94550

%D 2006

%G 1-878109-39-1

%I Fred Cohen and Associates

%O U\$24.00/C\$27.97 925-454-0171 all.net

%O [http://www.amazon.com/exec/obidos/ASIN/1878109391/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/1878109391/robsladesinterne)

<http://www.amazon.co.uk/exec/obidos/ASIN/1878109391/robladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/1878109391/robladesin03-20>

%O Audience n+ Tech 2 Writing 3 (see revfaq.htm for explanation)

%P 46 p.

%T "Information Security Awareness Basics"

This booklet is written as an employee security awareness manual. It can be purchased and used as such (by a small business), or customized and augmented by other materials (for a large enterprise). (If you intend using the primer "as is" for your employee manual, note that you should read it first, and ensure that you do, in fact, provide the services, and have the policies, that Cohen recommends. This should not be onerous, as the procedures outlined are quite reasonable, for any but the smallest business.)

The content is well-written, readable and clear, and covers a number of basic points that are often neglected (such as the importance of reading and understanding the contract with the employer, and, by extension, the employer's policies.) (The topics are approximately one page in length, or less, and are all, with one exception, on separate pages.) A significant portion of the early material is concerned with personal physical (rather than information) security. This is a very good arrangement, not only because it demonstrates concern for the well-being of the employee, but also since it starts with the more familiar (less esoteric) matters, and is a

good lead-in to the concepts of information security.

Well thought out, well written, and clear. This is a useful item for those who do not have the time to create their own security awareness materials, and a model for those who do.

copyright Robert M. Slade, 2007 BKINSCAB.RVW 20070119
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<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

Search RISKS using [swish-e](#)

Volume 24: Issue 66

Monday 14 May 2007

Contents

- [Browns Ferry 3 nuclear power site scrambled](#)
[PGN](#)
- [Reactors, remotely defended](#)
[Wendell Cochran](#)
- [Unit confusion caused fatal chemotherapy overdose](#)
[Mark Brader](#)
- [Error in climate data recording software](#)
[Charles Perrow via Martyn Thomas](#)
- [Another sat-nav accident: car destroyed, driver escapes](#)
[Mark Brader](#)
- [Touch typing](#)
[Jim Horning](#)
- [NZ fisheries "ruler" short](#)
[George Michaelson](#)
- [TSA Loses Hard Drive With Personal Info](#)
[PGN](#)
- [Internet2 Knocked Out By Homeless Man?](#)
[Chris Hodge via Dave Farber](#)

- [Ed Felten: You Can Own an Integer Too - Get Yours Here](#)
[Monty Solomon](#)
 - [More on the bogus Canadian "spy coin"](#)
[Jim Horning](#)
 - [Re: Impossible data requested](#)
[Gillian Brent](#)
 - [Re: Automatic translation leads to ethnic slur](#)
[Tony Ford](#)
 - [An interesting phishing risk...](#)
[Craig DeForest](#)
 - [Microsoft sets the wrong time in the PC's real time clock chip](#)
[Len Spyker](#)
 - [Re: US Daylight Saving Issues](#)
[Nick Bender](#) [John Levine](#) [Joseph Barrett](#)
 - [First Usenix Workshop on Offensive Technologies: WOOT 07](#)
[Tal Garfinkel](#)
 - [Info on RISKS \(comp.risks\)](#)
-

🔥 Browns Ferry 3 nuclear power site scrambled

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

Tue, 8 May 2007 10:58:28 PDT

This is another example of a system environment in which components that were supposedly not safety related could compromise safety. The case is of considerable interest to RISKS.

On 19 Aug 2006, operators manually scrambled Browns Ferry, Unit 3, following a loss of both the 3A and 3B reactor recirculation pumps, as required after the loss of recirculation flow -- which placed the plant in a high-power, low-flow condition where core thermal hydraulic stability

problems may exist at boiling-water reactors (BWRs). Generally, intentional operation is not permitted under this condition. Although some BWRs are authorized for single loop operation, sudden loss of even one pump could present the plant with the same stability problems and could result in the reactor protection system initiating a shutdown of the plant. [Source: Effects of Ethernet-based, Non-safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations, United States Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, DC 20555-0001, 17 Apr 2007; PGN-ed, although the following text is abridged but unedited.]

<http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2007/in20075.pdf>

The initial investigation into the dual pump trip found that the recirculation pump variable frequency drive (VFD) controllers were nonresponsive. The operators cycled the control power off and on, reset the controllers, and restarted the VFDs. The licensee also determined that the Unit 3 condensate demineralizer controller had failed simultaneously with the Unit 3 VFD controllers. The condensate demineralizer primary controller is a dual redundant programmable logic control (PLC) system connected to the ethernet-based plant integrated computer system (ICS) network. The VFD controllers are also connected to this same plant ICS network. Both the VFD and condensate demineralizer controllers are microprocessor-based utilizing proprietary software.

The licensee determined that the root cause of the event was the

malfunction

of the VFD controller because of excessive traffic on the plant ICS network.

Testing by site personnel performed on the VFD controllers confirmed that

the VFD control system is susceptible to failures induced by excessive

network traffic. The threshold levels for failure of the VFD controllers due

to excessive network traffic, as determined by the on-site testing, can be

achieved on the existing 10-megabit/second network. The NRC staff's review

of industry literature and test reports on network device sensitivity, and

the threshold levels for such failures, confirmed these testing results. The

licensee could not conclusively establish whether the failure of the PLC

caused the VFD controllers to become nonresponsive, or the excessive network

traffic, originating from a different source, caused the PLC and the VFD

controllers to fail. However, information received from the PLC vendor

indicated that the PLC failure was a likely symptom of the excessive network

traffic.

To ensure that excessive network traffic will not cause future Unit 3 VFD

controller malfunctions, the licensee disconnected these devices from the

plant ICS network before restart. The licensee also disconnected the Unit 2

VFD controllers from the plant ICS network.

Licensee corrective actions included (1) developing a network firewall

device that limits the connections and traffic to any potentially susceptible devices on the plant ICS network and (2) installing a network

firewall device on each unit -- VFD controller and condensate

demineralizer

controller. The Browns Ferry Unit 3 event is discussed in

Licensee Event

Report 05000296/2006-002, dated October 17, 2006, Agencywide Documents

Access and Management System, Accession No. ML062900106.

The reason the licensee at Browns Ferry investigated whether the failure of

one device, the condensate demineralizer PLC, may have been a factor in

causing the malfunction of the VFD controllers is that there is documentation of such failures in commercial process control.

For instance,

a memory malfunction of one device has been shown to cause a data storm by

continually transmitting data that disrupts normal network operations

resulting in other network devices becoming locked up or nonresponsive. A

network found to be operating outside of normal performance parameters with

a device malfunctioning can effect devices on that network, the network as a

whole, or interfacing components and systems. The effects could range from a

slightly degraded performance to complete failure of the component or

system. Major contributors to these network failures can be the addition of

devices that are not compatible, network expansion without a procedure and a

overall network plan in place, or the failure to maintain the operating

environment for legacy devices already on the network.

While only non-safety related network devices became nonresponsive at Browns

Ferry Unit 3, it is important to protect both safety-related and non-safety

related devices on the plant network to ensure the safe operation of the

plant. The 19 Aug 2006, transient unnecessarily challenged the

plant safety systems and placed the plant in a potentially unstable high-power, low-flow condition. The potential safety implications for future similar events would depend on the type of devices that are connected to the plant ethernet. Careful design and control of the network architecture can mitigate the risks to plant networks from malfunctioning devices, and improper network performance, and ultimately result in safer plant operations.

✶ Reactors, remotely defended

<Wendell Cochran <atrypa@eskimo.com>>

Thu, 26 Apr 2007 20:01:22 +0100

In **The New York Times**, 25 Apr 2007, a headline (A22, National Edition) reads 'U.S. Takes Step to Address Airliner Attacks on Reactors'.

The agency was the Nuclear Regulatory Commission; its 'step' was to urge that reactor designers seek to mitigate the effects of suicide attacks 'to the extent practicable' -- rather than to aim for 'the capability to withstand the effects of an aircraft crash.'

'Mitigate' vs 'withstand' is being debated, with one mitigator among the commissioners citing difficulty in making cost-benefit analyses based on speculation about probabilities.

The story goes on to say 'By the time new plants are actually built, he added, the aircraft industry may have solved the problem by

installing
equipment to control planes remotely in case of hijacking.'

It may be that the commissioner does not read RISKS.

✶ Unit confusion caused fatal chemotherapy overdose

<msb@vex.net (Mark Brader)>

Thu, 10 May 2007 18:38:01 -0400 (EDT)

The Alberta Cancer Board has released a report into the death of patient

Denise Melanson last August due to an accidental overdose of the chemotherapy drug fluorouracil. The prescription gave the dosage as "5,250

mg (at 4,000 mg/m²) intravenous once continuous over 4 days" and then as

"baseline regimen 1,000 mg/m²/day = 4,000 mg/m²/4 days". The m² here

apparently refers to the total area of the patient's skin and explained how

the dose in mg had been calculated rather than how it was to be administered.

To administer the drug, a nurse loaded it into a portable infusion pump.

The drug label would have read "Final Concentration: 45.57 mg/mL; Dose: 5250

mg/4 days (1312.5 mg/24h); Rate: 28.8mL/24h (1.2mL/h)". The pump had

several options to program the rate of flow, but none of them involved a

rate per day. The nurse selected milliliters per hour, and recalculated the

rate herself, but forgot to convert days to hours, and typed in the number

for mL/day, which she saw on the label.

For some other drugs 28.8 mL/h would have been a plausible amount, but with fluorouracil it was fatal. Another nurse checked the arithmetic, partly mentally, and did not spot the error. The problem was only realized when the drug supply ran out, and then it was too late. The fact that the pump's user interface said "mL" when it meant "mL/h" cannot have helped.

The report summarizes the causes as: "miscalculation; opportunity for false confirmation on label; information required to program pump not part of medication administration record; double check process failed; complex workload and multitasking; no feedback from pump; and low knowledge of hazard."

This is not the first time this sort of thing has happened, and the report details some of the other ones as well as making recommendations for improved procedures.

News media reports:

<http://www.cbc.ca/cp/health/070508/x050819A.html>

<http://www.theglobeandmail.com/servlet/story/LAC.20070509.OVERDOSE09/TPStory/National>

Cancer Board report (PDF, and curiously marked "Privileged and Confidential"

on every page):

http://www.cancerboard.ab.ca/NR/rdonlyres/D92D86F9-9880-4D8A-819C-281231CA2A38/0/Incident_Report_UE.pdf

Error in climate data recording software

<Martyn Thomas <martyn@thomas-associates.co.uk>>

Thu, 03 May 2007 07:54:41 +0100

Charles Perrow noticed this:

From the latest Nature: 447, p 7140

In 2006, data from the array led a team of scientists to the surprising conclusion that the world's oceans had cooled during 2003 exceptionally warm years in terms of global surface temperature. The team published its findings in Geophysical Research Letters¹. Such apparent cooling was seized on by people keen to highlight the uncertainties in forecasts of global warming².

That cooling has now been shown to be an artefact. In some of the buoys -- they are manufactured in separate batches -- a software glitch caused the temperature and salinity data to be associated with the wrong depths. When the problem data are excluded from the analysis, the cooling trend drops below the level of statistical significance.

✶ Another sat-nav accident: car destroyed, driver escapes

<msb@vex.net (Mark Brader)>

Sat, 12 May 2007 01:05:30 -0400 (EDT)

Accepting satellite-navigation directions without sufficient thought has caused another accident. A young woman in Great Britain

followed its directions onto a country lane which was blocked by a gate. At first she thought it was a dead end, she said, but "the sat nav insisted it was the correct way so I opened it and drove through."

After the first gate there was a second one, so she got out to close the first gate and open the second one, apparently not thinking about why there might be two gates across a road, or why there was a sign saying to proceed "if the light is green". (None of the news reports I found says any more about that light than that the sign existed.)

And while she was out of her car, a train came along the tracks and demolished it.

http://news.bbc.co.uk/2/hi/uk_news/wales/south_west/6646331.stm
http://icwales.icnetwork.co.uk/0100news/0200wales/tm_headline=sat-nav-guides-driver-into-path-of-train&method=full&objectid=19083438&siteid=50082-name_page.html
<http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/05/11/nsatnav11.xml>
http://www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=453991&in_page_id=1770

Touch typing

<Jim Horning <Jim.Horning@sparta.com>>
Wed, 25 Apr 2007 11:50:10 -0700

I have long been a fluent touch typist. I consider Typing to have been the high-school course that has been most useful during my

professional career.

Early this year I started noticing increasing problems with my typing. Sometimes characters would be dropped. As many as half of them. When things got bad, even if I slowed down and typed a single character at a time, I lost quite a few. I was sometimes reduced to a mode of typing a character, seeing if it appeared on the screen, and then either typing it again or proceeding to the next character. I found this quite distressing.

Initially, I thought it might be my keyboard, since I'd fairly recently acquired a new ergonomic keyboard. However, swapping the old keyboard back in didn't help.

I thought maybe I'd done something to mess up my software configuration, but checking all the settings I could think of that might be relevant didn't turn up anything out of the ordinary, and none of the changes I tried seemed to help. (Deleting Temporary Internet Files did sometimes seem to help a little bit, as did exiting Internet Explorer and restarting it.)

I found that I had the same problem on both my home and office computers, which made it seem unlikely that it was a problem with my hardware.

The problem seemed most acute when using Blogger, but checking the Help and searching the Web turned up no indication that anyone else was seeing this problem with Blogger. And it didn't only happen when I was using Blogger.

By this time I had to consider the possibility that the common factor was me. My neurologist ran some tests, and concluded that this was NOT peripheral neuropathy affecting my fingers (although I did have a mild case of Carpal Tunnel Syndrome that cleared up very quickly wearing wrist splints at night).

The penny dropped yesterday during a frustrating session creating a new blog post: I realized that the typing problem had started when I converted to Internet Explorer version 7, with its feature of "tabbed browsing," which I rather like. I typically have four to ten tabs open at any given time, more when I'm looking for information and links to put into my blog posts. The troublesome combination was typing into an IE form (e.g., the Blogger editor) while having a large number of tabs open.

I quickly tested this by opening a second IE window with only a single tab for Blogger, leaving the other window on the screen with all its tabs still open. Glory be! I could touch-type at my old speed once again!

It appears that IE 7's input de-multiplexing routine is so inefficient that it can't reliably keep up with a couple of characters per second when there are more than about six tabs open, even on a dual-core Pentium D 3.40 GHz processor with a 1 GB memory! This seems so preposterous to me that I'm asking for other IE 7 users to do the experiment and let me know if they see the same thing; alternatively, perhaps someone else can offer me a better explanation.

[We have nothing to fear but Blogosphere. FDR-PGN]

⚡ NZ fisheries "ruler" short

<George Michaelson <ggm@apnic.net>>

Mon, 7 May 2007 17:46:15 +0300

The New Zealand fisheries ministry handed out printed "rulers" to stick on the edge of a boat, to have handy for measuring fish sizes. (If too small, throw it back.) Unfortunately, the rulers were 20mm short.

<http://www.abc.net.au/news/newsitems/200705/s1916683.htm>

I'm wondering, with ABSOLUTELY NO EVIDENCE, given how print/production cycles work nowadays, whether this maybe could have been a PDF file at some point in its life, and that somebody forgot to un-check the option "shrink to fit". Or, something close.

⚡ TSA Loses Hard Drive With Personal Info

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

Tue, 8 May 2007 16:48:46 PDT

The U.S. Department of Homeland Security's Transportation Security Administration reported that it had lost a portable computer hard drive containing Social Security numbers, bank data, and payroll information for

about 100,000 employees from Jan 2002 to Aug 2005.

[Source: AP item in *The New York Times*, 5 May 2007]

http://topics.nytimes.com/top/reference/timestopics/organizations/t/transportation_security_administration/index.html?inline=nyt-org

⚡ Internet2 Knocked Out By Homeless Man? (via Dave Farber's IP)

<Chris Hodge <hodge@sunsite.utk.edu>>

May 2, 2007 11:42:02 PM EDT

<http://techdirt.com/articles/20070502/171657.shtml>

<http://www.networkworld.com/news/2007/050207-internet2-fire.html>

The news today is that a homeless man in Boston tossed a cigarette on a mattress, setting off a two-alarm fire that happened to knock out the Internet2 connection between New York and Boston.

⚡ Ed Felten: You Can Own an Integer Too - Get Yours Here

<Monty Solomon <monty@roscom.com>>

Tue, 8 May 2007 09:09:03 -0400

Ed Felten, 7 May 2007, <http://www.freedom-to-tinker.com/?p=1155>

Remember last week's kerfuffle over whether the movie industry could own random 128-bit numbers? (If not, here's some background: 1, 2, 3)

Now, thanks to our newly developed VirtualLandGrab technology, you can own a

128-bit integer of your very own.

Here's how we do it. First, we generate a fresh pseudorandom integer, just for you. Then we use your integer to encrypt a copyrighted haiku, thereby transforming your integer into a circumvention device capable of decrypting the haiku without your permission. We then give you all of our rights to decrypt the haiku using your integer. The DMCA does the rest. ...

✦ More on the bogus Canadian "spy coin" (Re: [RISKS-24.55,56,57](#))

<Jim Horning <Jim.Horning@sparta.com>>

Mon, 7 May 2007 18:33:00 -0700

The bogus report of Canadian "poppy quarters" with embedded radio-frequency transmitters apparently resulted because several different U.S. Army contractors traveling in Canada filed confidential espionage memos. The coins showed a red poppy overlaid on the Canadian maple leaf, where the red poppy had a protective coating that looked like a microscopic wire mesh "that looked like nano-technology." About 30 million coins were minted, commemorating Canada's 117,000 war dead. The AP managed to obtain redacted Secret NoForn government documents under the U.S. Freedom of Information Act. [PGN-ed]

http://news.yahoo.com/s/ap/20070507/ap_on_go_ot/spy_coins

[Ted Bridis article also noted by Kelly Bert Manning. PGN]

<http://www.cbc.ca/cp/Oddities/070507/K050723AU.html>

⚡ **Re: Impossible data requested ([RISKS-24.64](#))**

<reynardo@optusnet.com.au>

Fri, 20 Apr 2007 16:08:59 +1000

Residents of Australia have long known to add a fake 0 to the beginning of their 4 digit post code to allow ordering from US-centric online ordering companies.

But spend a moment in thought for the residents of Tristan da Cunha, in the middle of the Atlantic ocean, who only 2 years ago were allocated the UK post code (TDCU 1ZZ) to make it easier for the residents to order goods online.

(Information from Wikipedia, confirmed by other sources).

Gillian Brent, Matraville, NSW 2036

⚡ **Re: Automatic translation leads to ethnic slur (Epstein, [RISKS-24.65](#))**

<"Tony Ford" <tony.ford@ntlworld.com>>

Mon, 30 Apr 2007 18:51:01 +0100

The posting from Jeremy Epstein on 20 April illustrates a particularly egregious example. However, the fact remains that across the

world false
economies are constantly being made through commercially or
otherwise
important brochures, menus, product brochures, web pages etc
being
translated 'on the cheap'.

It seems that some businesses and organisations will persist in
shutting
their eyes to the impression that they make when they release
cringe-making
or even sub-standard translations of their flagship written
output.

The RISK is a reputational one, I guess: as they say, it takes a
long time
to establish a good reputation but it can be lost extremely fast.

(Here, although a computer translation program may have
facilitated the
event, at least it was not a case of GIGO.)

Tony Ford, Guildford, Surrey, UK

✶ An interesting phishing risk...

<Craig DeForest <deforest@boulder.swri.edu>>

Thu, 19 Apr 2007 17:06:39 -0600

Today, I received a call -- on my cell phone -- from a voice
synthesizer.

It claimed to be from my bank, and asked me to verify my
identify by typing
the last four digits of my social security number. Of course, I
hung up.

Since those four digits are so useful for authenticating all
manner of
bank-by-phone transactions, I can imagine a nice phishing

scheme: penetrate
an online store's customer database (thereby getting names,
phone numbers,
and credit card numbers -- which themselves contain bank
information) and
then autocalled every single one and ask for account passwords and/
or social
security numbers. Step 3: profit!

I wrote to my bank (Elevations Credit Union) expressing my
sincere hope that
it wasn't them, but I have a sinking feeling it was.

⚡ Microsoft sets the wrong time in the PC's real time clock chip

<Len Spyker <lspyker@helixesg.com>>

Mon, 14 May 2007 12:54:34 +0800

The MS design error and the risk:

Microsoft has always set your PC RTC (realtime clock chip) to
the "Local
Time" and not to UTC as unix and others do.

It then applies rules to correct that actual chips RTC time
(again and
again) during your daylight saving transitions.

This fundamentally broken idea results in a correction function
with two
possible time answers at the time shift boundary overlap.

Hence the ban on rebooting your PC multiple times in such an
overlap
period, as would force multiple time shifts!

However, if the RTC chip stored UTC and applied a UTC local time
offset

correction factor, then there is never ambiguity.

Even with VISTA WOW our wizards at Microsoft will apparently not fix this stupidity as no doubt it would break a few thousand apps.

⚡ Re: US Daylight Saving Issues ...

<"Nick Bender" <nbender@gmail.com>>

Thu, 26 Apr 2007 10:23:52 -0400

> I have no idea if the various patches I've applied to the systems I've been using have been applied only to the operating system, the C Run time libraries, or only half, and making sure that they are only applied once and not multiple times.

This is not likely a result of anything you have done.

DST under Windows (all versions) is fundamentally broken. The way they chose to implement the time change is to adjust **all** dates by one hour when DST is in effect.

Try this simple test:

1. Set your system time to the day before a time change.
2. Create a file and observe the timestamp.
3. Set your system time to the day after a time change.
4. Observe the timestamp on your file.

The time stamp will be one hour different after the time change.

This applies to **all** timestamps on **all** your files.

This also applies to **all** the entries in your event logs.

This is by design and is not likely to change. Ever.

This is a know problem (see <http://catless.ncl.ac.uk/Risks/22.35.html#subj10> for example).

> I think that this US DST switch is going to continually bite us in small
> ways for several years. The only solution I see is to operate computers on
> UCT without any time zone translation enabled, which isn't really a viable
> solution.

The first statement may be correct but not in the way you mean. The second statement is correct in general with respect to Windows systems.

I cannot say for certain not having looked at the code but I can only assume that products such as Outlook/Exchange which do calendaring which must be correct across time changes have entire libraries of code to deal with this issue outside of the standard Windows system libraries. Maybe someone who knows can enlighten the rest of us....

⚡ Re: US Daylight Saving Issues (Bonner, [RISKS-24.64](#))

<John Levine <johnl@iecc.com>>
26 Apr 2007 14:35:11 -0000

> ... the process should be data driven, through a configuration file.

All of the time conversion software I'm aware of these days is

indeed driven
by configuration files. But every time they change the DST
rules, the
config files have to change, leading to exactly the software
distribution
problems everyone has been noting.

John Levine, johnl@iecc.com, Primary Perpetrator of "The
Internet for Dummies",
Information Superhighwayman wanna-be, <http://www.johnlevine.com>,
ex-Mayor

✶ Re: US Daylight Saving Issues (Jones, [RISKS-24.65](#))

<Joseph <joseph_barrett@sbcglobal.net>>
Tue, 24 Apr 2007 22:59:46 -0700

Jones alleges that Microsoft keeps system clocks in UTC instead
of local
time (incorrect for versions 3.0, 3.1, 3.11 (WFW), 95, 95 OSR 2,
98, 98 SE,
NT 4.0, 2000, and XP); all of which set hardware clock to local
time, as
shown in BIOS.

The suggested use of UTC and a translation configuration file is
actually
typical of Unix/Linux/similar; not MS.

What risks do you see here?

✶ First Usenix Workshop on Offensive Technologies: WOOT 07

<"Tal Garfinkel" <talg@cs.stanford.edu>>
Tue, 1 May 2007 21:38:40 -0700

Got a good attack paper in the works?

In concert with the 2008 Usenix Security Symposium, we are putting on a Workshop On Offensive Technologies (WOOT). It is intended to pull in folks from a wide range of academic and industry communities to explore the state of the art in attack technologies in a high quality, peer reviewed setting.

Topics include:

- * Vulnerability research (software auditing, reverse engineering)
- * Penetration testing
- * Exploit techniques and automation
- * Network-based attacks (routing, DNS, IDS/IPS/firewall evasion)
- * Reconnaissance (scanning, software, and hardware fingerprinting)
- * Malware design and implementation (rootkits, viruses, bots, worms)
- * Denial-of-service attacks
- * Web and database security
- * Weaknesses in deployed systems (VoIP, telephony, wireless, games)
- * Practical cryptanalysis (hardware, DRM, etc.)

Submissions are due June 7th, check out the call for papers at:

<http://www.usenix.org/events/woot07/cfp/>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 67

Saturday 19 May 2007

Contents

- [E-stonia e-stoned](#)
[PGN](#)
- [Colorado State Government Computer Project Failures](#)
[Peter Shriner](#)
- [Alcatel-Lucent, lost disk](#)
[Ken Knowlton](#)
- [UK judge: "What's a website?"](#)
[Ken Knowlton](#)
- [BSoD forces students to retake standardized test](#)
[Jeremy Epstein](#)
- [Risks of combining too many cards](#)
[Jay R. Ashworth](#)
- [Information leak in combined systems](#)
[Paul E. Black](#)
- [Re: Touch typing](#)
[Jim Horning](#) [Tim Howe](#) [Martin Ward](#)
- [Re: Satellite navigation system](#)
[Ken Knowlton](#)

- [Re: Another sat-nav accident: car destroyed, driver escapes](#)
[Alan J. Wylie](#)
 - [Re: Daylight savings time and Microsoft](#)
[Bruce Dawson](#)
 - [Re: Time zones and MS Exchange and Outlook](#)
[Tony Finch](#)
 - [Re: Microsoft sets the wrong time in the PC's real time clock chip](#)
[Dag-Erling Smørgrav](#)
 - [Re: Felten, You Can Own an Integer Too - Get Yours Here](#)
[Mark Brader](#)
 - [Top 5 Reasons to Attend USENIX '07](#)
[Lionel Garth Jones](#)
 - [Info on RISKS \(comp.risks\)](#)
-

E-stonia e-stoned

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

Sat, 19 May 2007 12:38:39 PDT

In a demonstration of how a distributed denial of service attack can affect an entire nation, Estonian governmental computer systems have been under sporadic attacks this month, which later extended to newspapers, TV stations, schools, and banks in Estonia. Although many zombie systems appeared to have (presumably unsuspectingly) contributed to the attacks, Russian servers were involved, leading the Estonian government to suspect Russian complicity. The attacks intensified on 3 May (which coincided with protests in Moscow against the Estonian removal of a Soviet-era war monument) and again on 8-9 May (when Europe commemorates the end of World

War II). Russia denies complicity. [Source: Steven Lee Myers, Estonia Computers Blitzed, Possibly by the Russians, *The New York Times*, 19 May 2007; PGN-ed. The *NYTimes* article notes that Estonia is "a wired country that touts its paperless government and likes to call itself Estonia."]

[Various comments I have seen suggest that this may have been intended as an exploratory effort to see how effective such attacks could be, or perhaps a warning shot across the bow, rather than as an attack per se. The lack of ability for any definitive traceback on the Internet of course complicates analysis. The entire incident of course is illustrative of the potential for widespread disruption, and is therefore a case deserving serious study.]

Colorado State Government Computer Project Failures

<Peter Shriner <petershriner@yahoo.com>>
Wed, 16 May 2007 12:46:54 -0700 (PDT)

After spending six years in development and \$8 million dollars of state taxpayers' money, the new CSTARs registration system for Colorado's Department of Motor Vehicles apparently doesn't work. And it's just one of five major state computer projects worth \$325 million that have failed to meet expectations. CSTARs was contracted at \$10.3M.

There was ample warning. State and DMV staff said that their

efforts were basically ignored by state officials and the contractor, Avana. The state fired the subcontractor in charge of seeking their advice. Code was written before any detailed specifications. The state even suspended the development contract for a while in 2004.

[Source: Ann Imse, Doesn't compute: 'It's like you were having a baby, and it turned out ugly' New system to register motor vehicles just the latest to misfire for state, *Rocky Mountain News*, 16 May 2007; Long article starkly PGN-ed, but it is the full text should be no surprise to RISKS readers.]

http://www.rockymountainnews.com/drmn/local/article/0,1299,DRMN_15_5538977,00.html

⚡ Alcatel-Lucent, lost disk

<Ken Knowlton <KCKnowlton@aol.com>>

Sat, 19 May 2007 09:27:58 EDT

AP reports that Alcatel-Lucent has lost a disk containing names, addresses, SSN's, birthdates and salary data of thousands (on TV I heard 200,000) of employees, retirees and dependents [presumably including PGN and myself*].

<http://www.physorg.com/news98775487.html>

[And numerous other RISKS readers as well! PGN]

⚡ UK judge: "What's a website?"

<Ken Knowlton <KCKnowlton@aol.com>>

Fri, 18 May 2007 12:19:54 EDT

A JUDGE stunned a court yesterday by admitting he did not know what a WEBSITE was. Judge Peter Openshaw brought a shuddering halt to the trial of three men accused of internet terror offences as a witness was being quizzed about an extremist web forum. He told shocked prosecutors at Woolwich Crown Court, South East London: ``The trouble is I don't understand the language. I don't really understand what a website is.'' [Source: Tom Wells, *The Sun*, 17 May 2007]

<http://www.thesun.co.uk/article/0,,2-2007220614,00.html>

⚡ BSoD forces students to retake standardized test

<"Jeremy Epstein" <jepstein@webmethods.com>>

Wed, 16 May 2007 10:05:05 -0400

2900 Virginia students will have to re-take standardized tests because the computer systems failed during the testing process. There are two descriptions of what went wrong: the testing vendor "reported that there was a problem with a connection between two servers" and students' "computer screens suddenly turned blue and displayed an error message" (i. e., a BSoD). Whether this is one problem or two is unclear - but the RISKS of relying on systems that may not have been fully tested are pretty obvious. And in

addition to the stress for the kids (and the time taken away from instruction when they redo the tests), there's another factor - presumably, the retest date will have to use a different test, since the students have already seen some of the questions on the first shot. "State officials said there was an unrelated computer problem with online testing last week [where] 1,300 tests were interrupted and that the students will have to be retested."

The Standards of Learning (SOL) tests are how Virginia meets No Child Left Behind (NCLB). When it comes to actual learning, a more common usage for the acronym "SOL" is more appropriate, IMHO.

<http://www.washingtonpost.com/wp-dyn/content/article/2007/05/15/AR200705>

1502060.html

(free registration required)

⚡ Risks of combining too many cards

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

Fri, 18 May 2007 11:46:29 -0400

A thread was posted to Slashdot this week, about a proposal that's been floated to leverage the magstripe on some state driver licenses to make them into a debit/credit card as well.

I'm sure you can come up with some good reasons why that's RISKy, but you might be surprised to find out that quite a lot of the

postings on
the thread are well thought-ought and quite cogent, by RISKS
standards.

My two favorites:

1) It's illegal to give your driver license to anyone in many
states, but
you might want to lend your wife or child your debit card.

and

2) It used to be obvious to a robber that you had nothing worth
taking, if
all you were carrying was a DL. Now, though, that DL **might** be
a debit
card... and they'll have to take **you**, too, to have the PIN at
an ATM.

That latter one, to me, is enough to **outlaw** this practice,
whether the
vendor who's implementing it likes that or not. But what do I
know...?

<http://yro slashdot.org/article.pl?sid=07/05/17/2345231>

Jay R. Ashworth, Designer, Ashworth & Associates, St Petersburg
FL USA
+1 727 647 1274 <http://baylink.pitas.com> jra@baylink.com

Information leak in combined systems

<"Paul E. Black" <p.black@acm.org>>

Fri, 18 May 2007 12:53:29 -0400

A friend is getting married. As many of you have, I went to the
web site of
the store where they registered and selected some gifts. When I

checked
out, I got the following (identifying and unimportant details
elided.)

SHIP TO
***** her ***** and ***** him *****

YES! We have their shipping address on file.

(... items, prices, shipping, taxes, and total ...)

CARRIER : UPS TRACKING NUMBER :
1Z1V0*****

Although once upon a time, stores did list shipping address,
they don't now,
probably for privacy. However, when I later looked up the
tracking number,
UPS provided quite a few details about where the package went.

I got a chuckle to think I could "buy" addresses for only a two
dollar
butter knife, plus shipping and handling.

✉ **Re: Touch typing (Horning, [RISKS-24.66](#))**

<"Jim Horning" <Jim.Horning@sparta.com>>
Thu, 17 May 2007 15:45:42 -0700

Thanks to several readers, some more pieces of the puzzle seem
to be falling
into place. I now think that the problem was probably not due
to tabs, per
se, but to the cumulative amount of JavaScript executed during a
window's
lifetime. With tabs, everything gets concentrated into one
window, and the
window tends to stay around longer.

Steve Weeks <sweeks@sweeks.com>:

I've observed lossage with FireFox in the past. The problem wasn't as bad as yours. I usually have about 5 tabs open, but I don't know if that is related. Browser JavaScript implementations are very slow, and I think that's part of the problem, since all these new Ajax sites are using lots of JavaScript.

Thomas ten Cate:

I once was unable to type at all in Opera. Turned out that my characters were sent to a Java applet in a background tab. Perhaps you could investigate whether it matters if you have any Java or Flash stuff open in your background tabs?

Skip La Fetra <skip.lafetra@hp.com>:

This note of yours is consistent with other experience I have... The specific pages that have been most problematic have been very JavaScript-intensive.

Robert Scheidt <scheidt@skynet.be>:

I had a similar problem with IE7 and multiple tabs open. Not with typing but I noted that other applications would run very slowly when I had IE7 open. Looking at the task manager I found out that IE7 was using 100% of CPU. This could also cause the typing problems.

After running a registry cleaner it was fixed. I used "regseeker" which can be downloaded for free at hoverdesk.net. I am however not

100% sure

it was the registry cleaning which fixed it. At the same time I had

problems with Adobe's Flash player (used for more video's on the web). I

had to remove the Flash player with a utility available at Adobe's site

and reinstall Flash player. I ran the registry cleaner after that and I

noticed that it had detected a number of invalid activeX controls related

to previous versions of Flash player.

Keith Power <keith.power@gmail.com>:

I've noticed similar odd behaviour lately too, but I've narrowed mine down

to particular applications. So far, they're always "Web 2.0" apps, that

is, applications involving AJAX.

My biggest complaints are with Google's Gmail and Google's Code Hosting

(GCH), in both Opera and IE, since these are two sites I use regularly. Most of the time when I press backspace in Code it takes off

two characters instead of the one. And in Gmail, in the to field if Gmail

automatically enters an address and I press backspace to remove the

superfluous comma it always enters, it skips over the comma instead of

deleting it.

Any JavaScript experts out there who could further clarify the situation?

P.S. The most common suggestion I received was "Switch to FireFox."

Re: Touch typing (Horning, [RISKS-24.66](#))

<Tim Howe <vsync@quadium.net>>

Tue, 15 May 2007 01:18:38 -0400

With regard to Jim Horning's issues with Internet Explorer 7, may I point out that Opera and Firefox have had tabbed browsing for quite some time, seem to have worked most of the kinks out, and do at least allow typing at more than 10words/min.

Re: Touch typing (Horning, [RISKS-24.66](#))

<Martin Ward <martin@gkc.org.uk>>

Wed, 16 May 2007 09:50:44 +0100

The last time I encountered this problem was about 25 years ago with an accounts package running on a Commodore PET where you had to type the account code fairly slowly in order for the CPU to keep up.

The CPU in question was a 1MHz eight bit processor, the 6502, with 96 KB of RAM: so your Pentium is around 3,400 times faster, with over 10,000 times as much memory ... and four times as many bits!

"The most amazing achievement of the computer software industry is its continuing cancellation of the steady and staggering gains made by the computer hardware industry..."-- Henry Petroski

martin@gkc.org.uk <http://www.cse.dmu.ac.uk/~mward/>

G.K.Chesterton web site: <http://www.cse.dmu.ac.uk/~mward/gkc/>

✉ Re: Satellite navigation system ([RISKS-24.66](#))

<Ken Knowlton <KCKnowlton@aol.com>>

Mon, 14 May 2007 17:25:14 EDT

Just recently, as a passenger, I was introduced to the wonders of a satellite navigation system. I was quite delighted with the delicacy and precision of its micro-management as we exited a residential neighborhood, and eventually got out into the the bustling world. I could so easily have been lulled into "leaving the driving" to that gentle but assertive guarding angle. But ...

"stay in the left lane" (just do it)

"turn left in 500 yards" (slow down a bit now)

"turn left in 200 yards" (really slow down now)

"turn left" (this is it, TURN LEFT!)

Whoops! It's heavy traffic both ways, and NO-TURNS here except by a jug handle. No, we didn't turn and, perhaps fortunately, hadn't even slowed down. The disembodied voice immediately noticed, forgave our disobedience and, thinking aloud but clearly unperturbed, intoned "course re-computation" ... I cannot begin to enumerate the RISKS.

✉ Re: Another sat-nav accident: car destroyed, driver escapes

<"Alan J. Wylie" <alan@wylie.me.uk>>

Mon, 14 May 2007 22:30:02 +0100

This has nothing to do with sat-navs, and everything to do with driver stupidity.

The Western Telegraph has an article on the incident, with a high resolution photograph showing all the road signs on the approach to the crossing:

<http://www.westerntelegraph.co.uk/display.var.1224413.0.0.php>
http://www.westerntelegraph.co.uk/_images/db/42/91/LEVELCROSSING1.429125.full.jpg

Not quite fully visible in the photograph is a sign that reads:

- * Check that green light shows
- * Open *both* gates
- * Check that green light *still* shows
- * Cross *quickly*
- * Close both gates

<http://www.rail-reg.gov.uk/upload/pdf/rspg-2e-levxngs.pdf>

Page 66

Here is the section of the Highway Code dealing with level crossings:

<http://www.highwaycode.gov.uk/26.htm#265>

Some crossings have 'Stop' signs and small red and green lights. You MUST

NOT cross when the red light is showing, only cross if the green light is

on. If crossing with a vehicle, you should

- * open the gates or barriers on both sides of the crossing
- * check that the green light is still on and cross quickly
- * close the gates or barriers when you are clear of the crossing.

Note the explicit mention of "both sides of the crossing"

Here is the sign for a level crossing, clearly visible in the picture in the Western Telegraph report.

<http://www.highwaycode.gov.uk/signs05.htm>

<http://www.highwaycode.gov.uk/sign117.htm>

The upper sign is "risk of grounding":

<http://www.highwaycode.gov.uk/sign115.htm>

Knowledge of the highway code is required of all drivers, and a written examination on it is part of the UK driving test.

Alan J. Wylie <http://www.wylie.me.uk/>

* * * * Note added Wed, 16 May 2007 18:23:40 +0100

A discussion in the newsgroup uk.railway has revealed further interesting information.

See the thread following on from the posting

Message-ID: <SOETzQo6lGSGFAAb@perry.co.uk>
<<http://groups.google.co.uk/group/uk.railway/msg/ec4b544a942994a0>>

1) The picture in the Western Telegraph is not the view that the driver saw
- she was heading north. Images of this are at
<http://www.wjm.clara.net/ffynnongain/>

The separation between the level crossing sign and the crossing itself is much more than it appears in the long focal length shot in the Western Telegraph.

2) The official UK government document
<<http://www.rail-reg.gov.uk/upload/pdf/rspg-2e-levxngs.pdf>>

describes this type of crossing as a "User Worked Crossing" and states
"129. This type of crossing is only applicable where the railway crosses a private road".

The crossing is at the centre of this map:

<http://getamap.ordnancesurvey.co.uk/getamap/frames.htm?mapAction=gaz&gazName=g&gazString=SN264175>>

On the map the road does not appear to be private, and posters to the newsgroup who have visited the area state that they think it is a normal public highway.

3) Heading west along the A40, and then at St. Clears turning off it to head north-west to Hebron, there is a complicated limited access junction, which requires a driver to go almost 360 degrees round a roundabout and head back the way they had come to join the "B" road which is the obvious route, rather than the unclassified road on which the incident occurred.

<http://getamap.ordnancesurvey.co.uk/getamap/frames.htm?mapAction=gaz&gazName=g&gazString=SN274160>>

This may have confused the Sat-Nav system.

Re: Daylight savings time and Microsoft

<"Bruce Dawson" <brucedawson@cygnus-software.com>>
Tue, 15 May 2007 22:21:29 +0100

There have been two recent letters to Risks (<http://catless.ncl.ac.uk/Risks/24.66.html#subj16.1> being the

most recent)
complaining about how Microsoft implements DST and saying, as if
it is
obvious, that Microsoft is wrong ("fundamentally broken" was one
quote). They don't, however, waste anytime exploring the
alternatives and
their problems.

As Nick Bender says, when you change to daylight savings time
then Windows
displays all of your file timestamps using daylight savings
time, even those
that were created outside of daylight savings time. This is a
good thing,
for many reasons:

If you create a file, and then an hour later create another file
then
Windows will show their time stamps as being an hour apart,
always. If the
'current wall clock time when they were created' is used instead
then these
two files might have times that are an hour apart, or they might
have times
that are two hours apart (in the spring) or they might both have
the same
time stamp (in the fall)! In order to display these times
unambiguously you
would need to display the time-zone, so that instead of:
 readme.txt 5:00 pm
you would need:
 readme.txt 5:00 pm EDT

Even if Windows did this, all is not happy and consistent. If I
am in
Seattle and I create a file at 5:00 pm then it will show a
timestamp of 8:00
pm when I am in New York. According to the ambitious 'show
creation time'
strategy this file should show 5:00 pm PST (or PDT) as its
creation
time. That sounds nice, but not very likely, and without that
the proposed

'solution' seems incomplete.

Another problem is that daylight savings time rules vary by year and by location. The UK started daylight savings time two weeks after the US. Some states within the US don't use daylight savings time. Some countries (crazy Australians) use daylight savings time during what we call winter! So how, I want to know, is Windows supposed to know whether daylight savings time was in effect when a file was created? Unless it records that fact at creation time then it cannot display the 'local creation time'. Recording the local time zone at creation time is not possible for a host of compatibility reasons.

The Win32 rules are not perfect for all cases, but they make perfect sense in many contexts. Changing this behavior, in addition to the backwards compatibility implications, would just trade one set of problems for another.

Raymond Chen covered this in his blog in October 2003, where he also points out that .NET does it differently.

<http://blogs.msdn.com/oldnewthing/archive/2003/10/24/55413.aspx>

⚡ Re: Time zones and MS Exchange and Outlook

<Tony Finch <dot@dotat.at>>

Mon, 14 May 2007 21:57:19 +0100

Nick Bender <nbender@gmail.com> wrote:

>

> I cannot say for certain not having looked at the code but I can only assume

> that products such as Outlook/Exchange which do calendaring which must be

> correct across time changes have entire libraries of code to deal with this

> issue outside of the standard Windows system libraries. Maybe someone who

> knows can enlighten the rest of us....

The process that sysadmins managing Exchange servers had to go through

to deal with the US DST rule change was astonishing. It revealed a

catastrophically wrong-headed database design. All the data in the

Exchange database had to be scanned and re-written to fix incorrect

timezone offsets stored in appointments that were to happen in the

period between the new and old offset changes. Utterly brain-damaged.

<http://support.microsoft.com/?kbid=930879>

⚡ Re: Microsoft sets the wrong time in the PC's real time clock chip

<des@des.no (Dag-Erling Smørgrav)>

Tue, 15 May 2007 11:31:28 +0200

(Spyker, [RISKS-24.66](#))

> ... as no doubt it would break a few thousand apps.

It would break absolutely nothing, since apps get their time from the

operating system, not from the BIOS RTC (which they cannot access anyway;

attempting to do so would trigger a general protection fault).
The only
issue would be having to set your clock when upgrading from a
Windows
version that uses local time to one that uses UTC.

✉ Re: Felten, You Can Own an Integer Too - Get Yours Here ([RISKS-24.66](#))

<msb@vex.net (Mark Brader)>
Tue, 15 May 2007 00:07:03 -0400 (EDT)

> Remember last week's kerfuffle over whether the movie industry
could own
> random 128-bit numbers? (If not, here's some background: 1, 2,
3)

Yes, that certainly is some useful background there. Just
think, only
340,282,366,920,938,463,463,374,607,431,768,211,453 more terms
in the
series, and we start getting to 128-bit numbers!

But what I really want to know is, which one is now claiming
ownership of
1, 2, and 3 -- Ed Felten or Monty Solomon?

Mark Brader, Toronto, msb@vex.net

[Oh yeah: ROTFL! Risks of copying from a web browser, I
suppose. Those were
actually supposed to be links, of course -- to these pages by
the same author:

<http://www.freedom-to-tinker.com/?p=1152>

<http://www.freedom-to-tinker.com/?p=1153>

<http://www.freedom-to-tinker.com/?p=1154>

MB]

⚡ Top 5 Reasons to Attend USENIX '07

<Lionel Garth Jones <lgj@usenix.org>>

Fri, 18 May 2007 13:49:53 -0700

Top 5 Reasons to Attend the 2007 USENIX Annual Technical Conference

June 17-22, 2007, Santa Clara, CA

<http://www.usenix.org/usenix07/progb>

USENIX '07 offers a cost-effective, one-stop shop for the latest in IT

training, break-throughs, and systems research. Check out the top 5 reasons

to join us in Santa Clara, CA, June 17-22, 2007:

1. Top-notch training: Highly respected experts provide you with new information and skills you can take back to work tomorrow. Topics include:

- Richard Bejtlich on TCP/IP Weapons School, Layers 2-3
- Peter Baer Galvin on Solaris 10 Security Features
- AEleen Frisch on Administering Linux in Production Environments
- Steve VanDevender on High-Capacity Email System Design

To view the entire training program, see:

<http://www.usenix.org/events/usenix07/training>

2. Invited Talks that feature industry luminaries discussing timely and important topics, such as:

- Keynote Address by Mendel Rosenblum of Stanford University, "The Impact of Virtualization on Computing Systems,"
- Plenary Closing by Mary Lou Jepsen, One Laptop per Child, "Crossing

the Digital Divide: The Latest Efforts from One Laptop per Child"

-- Rob Lanphier, Linden Lab, "Second Life"

<http://www.usenix.org/usenix07/ITs>

3. You'll see it here first:

-- The latest developments in cutting-edge systems research in the

Refereed Papers track.

<http://www.usenix.org/events/usenix07/tech>

-- An introduction to interesting new or ongoing work at the Poster Session.

<http://www.usenix.org/events/usenix07/activities.html#poster>

4. Answers to your toughest questions:

-- Guru Is In sessions feature experts who come prepared to respond to your

most burning technical questions on hot topics. The full list of topics

will be announced soon!

<http://www.usenix.org/events/usenix07/tech>

5. The chance to mingle with industry leaders:

-- Evening events such as the Birds-of-a-Feather (BoF) sessions offer

additional opportunities to network with peers to gain that all-important

"insider" IT knowledge.

<http://www.usenix.org/events/usenix07/bofs.html>

And that's just the beginning. Visit <http://www.usenix.org/usenix06/progb> to

see the full list of offerings.

Don't forget:

-- Register at the headquarters hotel by May 29, 2007, to

receive the
discounted hotel room rate:

<http://www.usenix.org/events/usenix07/hotel.html>

-- Register by June 1 and save up to \$300!

<http://www.usenix.org/events/usenix07/registration>

-- Take advantage of the multiple employee discount for groups
sending 5
or more:

<http://www.usenix.org/events/usenix07/registration/#multi>

2007 USENIX Annual Technical Conference

June 17-22, 2007, Santa Clara, CA

<http://www.usenix.org/usenix07/progb>

Early Bird Registration Deadline: June 1, 2007



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 68

Monday 11 June 2007

Contents

- [US Flight Service Privatization system problems](#)
[Don Poitras](#)
- [FDA issues Class I recall for an algorithm](#)
[Richard Cook](#)
- [New Hampshire federal judge overrules privacy law](#)
[Ethan Ackerman](#)
- [IT industry has failed in desktop security](#)
[Munir Kotadia via PGN](#)
- [Belgian biometric passport](#)
[Jean-Jacques Quisquater](#)
- [Flawed Symantec update cripples Chinese PCs](#)
[PGN](#)
- [Facebook doesn't allow friends born before 1910](#)
[Henry Baker](#)
- [Royal Bank of Scotland total failure of cash access systems](#)
[PGN](#)
- [Keyloggers used to steal city funds](#)
[Rick Damiani](#)

- [Want to Write a Virus? Take a Class](#)
[Erik Larkin via George Ledin](#)
 - [Windows' ATMs](#)
[Mark Barnabas Luntzel](#)
 - [Round Up, Round Down, or How one cent became a profitable event](#)
[Leon Kuunders](#)
 - [Re: UK judge: "What's a website?"](#)
[Rob Slade](#)
 - [Re: Broken Microsoft + Daylight saving](#)
[Len Spyker](#)
 - [Engaging Privacy and Information Technology in a Digital Age](#)
[Jim Horning](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈ US Flight Service Privatization system problems

<Don Poitras <poitras@pobox.com>>

Thu, 24 May 2007 08:36:48 -0400 (EDT)

Lockheed Martin has been converting Flight Service Stations (FSSs) to use new software and digital interfaces to FAA computers since it won the contract to run the stations in 2005. Part of the contract were guarantees that certain response times were achieved. Phone calls were to be answered in 20 seconds, radio calls answered with 5 seconds and flight plans filed within 3 minutes.

With the start of fair-weather flying by the majority of US private pilots this spring, the system has come under stress and response times have been abysmal, flight plans have been dropped and weather briefings have been

conducted by briefers with no local knowledge of weather conditions.

CONTROLS OVER THE FEDERAL AVIATION ADMINISTRATION'S CONVERSION OF FLIGHT

SERVICE STATIONS CONTRACT OPERATIONS

<http://www.oig.dot.gov/item.jsp?id=2051>

"Several FAA officials indicated that the use of call off-loading has increased significantly since the contract was put in place. In some cases, we found multiple facilities that had to adjust their operations in order to cover off-loaded calls from short-staffed facilities, which created a cascading effect across the country."

and:

"FS-21 requires digital capabilities and, per terms of the contract, must interface with FAA's Telecommunications Infrastructure Network. To meet this requirement, FAA plans on installing digital connections between the Lockheed Martin hub facilities and the closing and continuing flight service stations. While FAA has begun installing the digital connections, one FAA official noted that, based on the current schedule, there are only about 75 days between when the digital connections are installed and when operations at closing and continuing flight service stations are cut over. Given the tight timeframe, any delays or problems with the installation of these connections could hamper testing and operation of FS-21, possibly delaying the transition and increasing contractual costs."

AOPA's (Aircraft Owners and Pilots Association) Phil Boyer had

this
to say:

"In short, the FS21 (twenty-first century) system is in crisis and failing

pilots. Based on the hundreds of complaints that AOPA has received in the

past month, it is clear that the technical and operational problems

plaguing FS21 are now affecting safety," said AOPA President Phil Boyer in

a letter to FAA Administrator Marion Blakey. "The FAA and Lockheed Martin

must immediately address the problems and implement a plan to bridge the

service gap and provide critical FSS safety of flight services."

There are several safety issues. If the automated system ends up sending you

to a weather briefer in another state, he might not be aware of local

conditions, e.g., wind coming over a local mountain might produce severe

turbulence, but he wouldn't know that and wouldn't have any reason to

mention it.

A more serious safety risk is just that pilots may avoid getting pre-flight

briefings altogether because they can't get through.

Personally, (and the reason I'm making this post) I was trying to get an IFR

clearance and ended up getting bounced around the system and ended up with a

briefer in Macon, GA (I'm in Raleigh, NC). He had to fumble through what was

obviously a labor intensive effort to get the call switched to Raleigh. While talking to Raleigh, the call disconnected.

As I was going through this, the plane behind me was doing the same thing.

After about ten minutes he says to me (via the radio), "I'm on hold, the ASOS (automated local weather recording) says 1500 feet, so I'm going VFR."

I ended up doing the same thing. Leaving VFR in marginal conditions means that ATC will not be providing IFR separation services. They don't even know you've left until you call them up. Well, they might see your VFR transponder code, but they won't have any idea where you're going.

✶ FDA issues Class I recall for an algorithm

<Richard Cook <ri-cook@uchicago.edu>>

Wed, 06 Jun 2007 06:59:20 -0500

> Date: Tue, 5 Jun 2007 13:01:43 -0400
> From: CDER MEDWATCH LISTSERV <MEDWATCHLIST@CDER.FDA.GOV>
> Subject: FDA - MedWatch- Alcon Refractive Horizons LADAR6000
Excimer
> Laser System Class I Recall Because The Algorithm For Myopia
With and
> Without Astigmatism Caused Cornea Abnormalities
>
> MedWatch - The FDA Safety Information and Adverse Event
Reporting Program
>
> Alcon Refractive Horizons and FDA notified healthcare
professionals and
> patients of a Class I Recall of the LADAR6000 Excimer Laser
System for
> CustomCornea algorithm for myopia with astigmatism (M3) and
myopia
> without astigmatism (A7). This system is used for LASIK and
wave-front
> guided LASIK treatment for the reduction or elimination of
mild to

> moderate nearsightedness (myopia) and farsightedness
(hyperopia) with or
> without astigmatism or for mixed astigmatism in patients who
are 21
> years of age or older with documented stability of refraction
for the
> prior 12 months. The product was recalled because use of the
Alcon
> Refractive Horizons CustomCornea algorithm for myopia with and
without
> astigmatism with the LADAR6000 Excimer Laser caused corneal
> abnormalities ("central islands") and decreased visual
sharpness (visual
> acuity) in patients with myopia with and without astigmatism.
These
> "central islands" may not be correctable with lasers and the
decrease in
> visual acuity may not be correctable with glasses or contact
lenses.
> Patients with questions should call the company at 1-877-523-
2784.
>
> Read the complete 2007 Safety Summary, including a link to the
FDA
> Recall Notice regarding this issue at:
>
> <http://www.fda.gov/medwatch/safety/2007/safety07.htm#LADAR6000>

Recalling an algorithm is a relatively new phenomenon. Devices
such as
infusion pumps typically have firmware and software that is
integral to the
device. Complex devices such as LASIK systems allow the operator
to select
amongst multiple functions using different algorithms. In
February of this
year, Alcon told customers to stop using two algorithms (M3 and
A7) and went
on to 'deactivate' these algorithms in U.S. devices. A Class I
recall is
for "dangerous or defective products that predictably could
cause serious
health problems or death. Examples of products that could fall

into this category are a food found to contain botulinal toxin, food with undeclared allergens, a label mix-up on a life saving drug, or a defective artificial heart valve."

Richard I. Cook, MD, University of Chicago, Anesthesia and Critical Care,
Chicago IL 60637 1-773-702-4890 <http://www.ctlab.org/Cook.cfm>

✦ New Hampshire federal judge overrules privacy law

<Ethan Ackerman <eackerma@u.washington.edu>>

May 22, 2007 5:30:43 PM EDT

1st Amendment protects reselling medical records. [via Dave Farber's IP]

The New Hampshire Legislature recently enacted a law that bars pharmacies, insurance companies, and similar entities from transferring or using both patient-identifiable data and prescriber-identifiable data for certain commercial purposes. The law was enacted to protect patient privacy, prescriber privacy, and to prevent drug industry 'targeting' of doctors who prescribed generics.

It was promptly challenged by 2 data-mining companies who buy up prescription records from pharmacies and resell the info to drug manufacturers, and on April 30th was overturned by US District Court Judge Paul Barbadoro.

Judge Barbadoro ruled that the data-miners had a 1st Amendment

right to
resell the prescription records and the State of New Hampshire
violated that
right in passing this law.

<http://www.washingtonpost.com/wp-dyn/content/article/2007/05/21/AR2007052101701.html>

has a "big picture" treatment of the issue which mentions the case.

It also looks like the state plans to appeal:

<http://www.citizen.com/apps/pbcs.dll/article?AID=/20070504/NEWS0201/70504029/-1/CITIZEN>

[IP Archives: <http://v2.listbox.com/member/archive/247/=now>]

✶ IT industry has failed in desktop security (Munir Kotadia)

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

Fri, 25 May 2007 13:54:55 PDT

The IT industry has failed when it comes to desktop security for all major operating systems. Ivan Krstic, director of security architecture for the One Laptop per Child project, kicked off the AusCert 2007 conference Monday morning with a keynote speech that blasted desktop computer security -- including that of Windows, Linux and Macintosh machines -- because it is based on a 35-year-old premise where software can run with the same privilege as a user. ... One example of such a program, he said, is Minesweeper <[http://en.wikipedia.org/wiki/Minesweeper_\(computer_game\)](http://en.wikipedia.org/wiki/Minesweeper_(computer_game))>, a single-player game that has shipped with virtually all versions

of Microsoft

Windows. [Source: Munir Kotadia, ZDNet AUStralia, Expert: IT industry has

failed in desktop security, *News.com*, 22 May 2007; PGN-ed]

http://news.com.com/Expert+IT+industry+has+failed+in+desktop+security/2100-1002_3-6185295.html

<http://www.zdnet.com.au>

🔥 Belgian biometric passport

<Jean-Jacques Quisquater <jjq@dice.ucl.ac.be>>

Sat, 09 Jun 2007 14:26:55 +0200

A research team in cryptography (Gildas Avoine, Kassem Kalach and Jean-Jacques Quisquater) from the Catholic University of Louvain (Louvain-la-Neuve) disclosed serious weaknesses in the Belgian biometric

passport, the only type of passport distributed in Belgium since the end of

2004. The work carried out in Louvain-la-Neuve during the course of May 2007

show that Belgian passports issued between end 2004 and July 2006 do not

include any security mechanism to protect the personal data embedded in the

passport's microchip. Passports issued after July 2006 do benefit from

security mechanisms but these ones are flawed. This means that anyone

possessing a little electronic reading device, which is easy and cheap to

acquire, can steal the passport content while it is still in the pocket of

the victim owners and thus without their knowing. Face and signature are

among the data at risk. This news is all the more surprising because Karel

De Gucht, the Belgian Minister for Foreign Affairs, declared in

the Belgian Parliament on 9th January 2007 that the Belgian passport benefited from the security mechanisms advocated by the International Civil Aviation Organization. Skimming (that is, reading remotely these passports without the consent of the holder) is thus very easy and is true for 720.000 passports valid till end 2009 at least, out of all 1.500.000 valid Belgian passports. [Probably gratuitous for most of you but note that Belgian "." = American ","]

The risk is evident for the privacy of their holders. From the obtained information such flawed passports are the only ones in the world.

More at <http://www.dice.ucl.ac.be/crypto/passport/index.html>

✶ Flawed Symantec update cripples Chinese PCs

<"Peter G. Neumann" <neumann@csl.sri.com>>
Thu, 24 May 2007 12:58:05 PDT

[TNX to Keith A Rhodes. PGN]

An erroneous Symantec antivirus signature update caused Norton Internet Security 2007 and Norton 360 antivirus software to identify two critical system files (netapi32.dll and lsasrv.dll) as the Backdoor. Haxdoo Trojan in the Simplified Chinese version of Windows XP (with Service Pack 2 and a particular patch), resulting in those files being quarantined. As a result, millions of PCs throughout China were crippled, unable to be rebooted. ``According to Symantec, the problem was caused when

Symantec made
a change to the automated process used by the company's security
response
team to detect malicious software.' ' [Source: Article by Aaron
Tan, CNET
News.com; PGN-ed]

http://news.com.com/Flawed+Symantec+update+cripples+Chinese+PCs/2100-1002_3-6186271.html?tag=st.ref.goo
<http://www.cctv.com/program/bizchina/20070524/103599.shtml>

🔥 Facebook doesn't allow friends born before 1910

<Henry Baker <hbaker1@pipeline.com>>

Thu, 24 May 2007 14:43:23 -0700

Facebook discriminates against centenarians! You can't get an
account
unless your birthday is 1910 or later. (Of course, most
centenarians won't
have the prettiest faces for Facebook, but everything is
relative...)

[According to Wikipedia, there are 55K centenarians in the US
and 25K in

Japan, so this is not a small market. I think that the
founder of

Facebook is about 23 years old, so perhaps he doesn't trust
anyone over

100. I've got 40 years before worrying about this, but I
don't want to

run into a Y2K-type problem with 100+ ages. (Actually, there
already is

such a problem, as many websites only allow 2 digit ages.) HB]

🔥 Royal Bank of Scotland total failure of cash access systems

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

Sat, 2 Jun 2007 11:58:13 PDT

The Royal Bank of Scotland (RBS), which also owns NatWest, has apologised after its cashpoint, online, and telephone banking systems all crashed. A spokeswoman said: "We are very sorry, and we're working to sort it out."

[Source: BBC, courtesy of Keith Rhodes; PGNed]

http://news.bbc.co.uk/nolpda/ukfs_news/hi/newsid_6714000/6714857.stm

⚡ Keyloggers used to steal city funds ...

<"Rick Damiani" <rick@patongroup.com>>

Fri, 1 Jun 2007 17:49:37 -0700

... \$450,000.00 in attempted wire transfers, but the city was able to freeze all but \$45,000.00. *LA Times*

<http://www.latimes.com/news/local/la-me-hackers1jun01,1,3026207.story?coll=la-headlines-california>

Interesting quote:

"Avilla said she still doesn't know how her computer was targeted. She said she doubts it had the latest security software patch protections - something sheriff's detectives and bank investigators told her is essential in safeguarding her computer."

Two-factor authentication wasn't mentioned, so my guess is that the city's

bank doesn't offer it or the city chose not to use it.

Rick Damiani, Applications Engineer, The Paton Group
California: (310)429-7095 Hawaii: (808)284-3033

Want to Write a Virus? Take a Class (Erik Larkin, *PC WORLD*)

<George Ledin <ledin@sonoma.edu>>

Tue, 22 May 2007 16:10:49 -0700

[Ironically, the story is spreading... like a virus! George]

<<http://blogs.pcworld.com/staffblog/archives/004452.html>>

Want to Write a Virus? Take a Class. Erik Larkin, 22 May 2007

A college computer course that teaches students how to write computer viruses is riling up security companies once again, according to a story in a local California paper today.

Per the story, a computer science professor [George Ledin] at Sonoma State University in California is teaching the course in order to train his students how to design better defenses. Security companies, on the other hand, have always vigorously decried any attempts to create new malware as automatically unethical, no matter the end goal. And at least three companies are sending Ledin letters saying they will boycott hiring Ledin's students, according to the story.

This is an ongoing debate.

<<http://www.informationweek.com/story/showArticle.jhtml?articleID=10100296>>

Other colleges have previously taught such classes, and Consumer Reports

took major heat when it created new malware to test antivirus software.

<http://blog.washingtonpost.com/securityfix/2006/08/antivirus_testing_and_consumer_1.html>

So who's right? Is Ledin violating an unwritten Hippocratic oath of computer security? Or is this an important thing to teach, and learn, and test?

Personally, I think the genie's out of the bottle. Unlike with biological viruses, it's not hard to create a new piece of malware. You don't need a lab, expensive equipment or even much techie know-how; There has long been software available that allows any aspiring online thug to easily create a new piece of malware.

What's more, malware writers are constantly spewing out new variants in an attempt to evade antivirus programs. The recent <<http://www.pcworld.com/article/id,130686-page,1/article.html>> Storm Worm blast was a great example.

So I don't really think it makes us less safe if a few students create new malware in order to learn how they're built. Even if one of them escapes its protected environment, it will be a drop in the bucket compared to the already existing deluge of new virus variants that come out all the time.

And such training may help with what's really important: Developing

<<http://www.pcworld.com/article/id,129883-page,2-c,antivirus/article.html>>

effective proactive defenses that can block attacks whether they're old or

brand new.

⚡ Windows' ATMs

<"Mark Barnabas Luntzel" <mark@luntzel.com>>

Mon, 11 Jun 2007 09:01:00 -0700

Here is a Russian ATM with a Windows Product Activation screen:

Your Windows product must be activated within 7 days.
Do you want to activate Windows now?

<http://www.geekologie.com/2007/06/11/russian-windows-atm.jpg>

⚡ Round Up, Round Down, or How one cent became a profitable event

<Leon Kuunders <leon@kuunders.info>>

Tue, 29 May 2007 09:32:47 +0200

One Dutch energy company, Eneco, offers an extra service to other organisations, they act as an collecting agent. My local cable television company Rekam is using that service to have their monthly payments collected. One of the invoices I received recently showed a to-be-collected amount of 5,01. I immediately got triggered by this number: where did this one cent originate from?

Quick research showed the cable company charges you with 5,00 for administration costs. Including 19% VAT. When the energy company

tried to
calculate the costs without VAT they got into a nasty problem:
the amount
excluding VAT comes down to 4,2016806722 .. etc. Rounded this
would be
4,20. When they calculated 19% VAT of 4,20, it equals 0,798.
Dutch taxrules
require to round down such a number to ... 0,79.

This would leave them with a total amount of 4,99. But hey! That
wasn't
enough! So they decided to round up the amount excluding VAT to
4,21 and
then calculate the 19% VAT: 0,7999. Then they decided that this
number was
close enough to round up to 0,80 (against dutch tax rules ...).
The total
amount then was $4,21 + 0,80 = 5,01$.

In a conversation with the general manager of the cable company
he ensured me
that there was no way around this, and offered to sent me a
direct bill of
15,00. Because they had outsourced their billing department they
had to
increase direct bills with •â,•¬ 10,00 administration costs. ...

The risks of this event are as follows: because the energy
company
automatically debits the accounts of their customers this one
cent will
automatically be transferred to their account. The cable company
does not
collect this amount, nor do they pay it to the dutch tax
services. So
somewhere somebody enjoys these orphaned one cent payments.

In the last letter I received from the cable company the general
manager told
me I could go to court to get this issue resolved. My lawyer has
confirmed
that that was the best news she had in years.

Re: UK judge: "What's a website?" (Knowlton, [RISKS-24.67](#))

<Rob Slade <rMslade@shaw.ca>>

Sat, 19 May 2007 17:14:26 -0800

(<http://www.thesun.co.uk/article/0,,2-2007220614,00.html>)

I can't really tell if this is a good thing or a bad. Possibly some of the evidence in regard to identity hangs on who accessed a website (or had ownership of it). In that case I would assume that a solid understanding of the technology would be necessary. A faulty understanding might result in an incorrect decision (as seems to be the situation with the Amero case in the US).

Certainly I can have sympathy with another comment in the story:

"Later he said he hoped a computer expert would give `simple' evidence

when called to the stand -- because otherwise he would not understand it.

"Judge Openshaw said: `Will you ask him to keep it simple? We've got to start from basics.'"

Being involved in certain aspects of forensics, I recognize that a number of

"experts" simply seem to want to be able to give an opinion without being

challenged, questioned, or having to explain their reasoning and opinions.

(Given the way the story is written, I can easily recognize the risks of admitting that you need help with technical concepts outside your field ...)

rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm> www.syngress.com/catalog/?pid=4150

✶ Re: Broken Microsoft + Daylight saving

<"Len Spyker Perth Australia" <lspyker@helixesg.com>>
Thu, 24 May 2007 13:21:53 +0800

Dag-Erling Sm=F8rgrav disagrees in [RISKS-24.67](#) to my stating in [RISKS-24.66](#) that fixing the Microsoft RTC design bug would break a few thousand apps.

He asserts that as only high level system calls are used and they would see no changes and all would be well.

While I agree in principle, reality was different.

I recently worked on a 6 months software project involving monitoring many mine sites and ports, in the middle of which our state government introduced daylight saving for the FIRST time ever, on barely 4 week notice.

We had the expected breaking of legacy boxes that had no notion of daylight saving, OK.

However the biggest surprise was the number of state of the art corporate

databases from well known global companies that broke badly.

They appeared to contain code fudges to work around the MS ambiguity and other problems I mentioned.

Some of these global databases had no sense of a UTC time stamp and used "local" time stamps only!

We uncovered a rat's nests of daylight or no daylight savings kludges at every system level by every vendor and applications writers that another \$500K barely made a dent in.

If you can't trust your OS high level system time calls 100.0% and you have to work around them, then it still doesn't help.

🔥 Engaging Privacy and Information Technology in a Digital Age

<"Jim Horning" <Jim.Horning@SPARTA.COM>>

Fri, 25 May 2007 13:03:42 -0700

This book <http://books.nap.edu/catalog.php?record_id=11896> will, I think, be of interest to many USACM members interested in IT privacy issues as viewed from a variety of perspectives outside our usual computer-oriented view. Now available for pre-order from the National Academies Press, it is the result of a multi-year study committee on Privacy in the Information Age (of which I was a member), sponsored by the Computer Science and Telecommunications Board (CSTB) of the National Research Council (NRC).

Privacy is a growing concern in the United States and around the world. The spread of the Internet and the seemingly boundaryless options for collecting, saving, sharing, and comparing information trigger consumer worries.

Online practices of business and government agencies may present new ways to compromise privacy, and e-commerce and technologies that make a wide range of personal information available to anyone with a Web browser only begin to hint at the possibilities for inappropriate or unwarranted intrusion into our personal lives. *Engaging Privacy and Information Technology in a Digital Age* presents a comprehensive and multidisciplinary examination of privacy in the information age. It explores such important concepts as how the threats to privacy evolving, how can privacy be protected and how society can balance the interests of individuals, businesses and government in ways that promote privacy reasonably and effectively? This book seeks to raise awareness of the web of connectedness among the actions one takes and the privacy policies that are enacted, and provides a variety of tools and concepts with which debates over privacy can be more fruitfully engaged. *Engaging Privacy and Information Technology in a Digital Age* focuses on three major components affecting notions, perceptions, and expectations of privacy: technological change, societal shifts, and circumstantial discontinuities. This book will be of special interest to anyone interested in understanding why privacy issues are often so intractable.

The full draft text is available free online
<http://books.nap.edu/catalog.php?record_id=11896>, and will be replaced
with the final version when it is published. Much credit is due to the
editors, Jim Waldo, Herb Lin, and Lynnette Millett for imposing a substantial amount of coherence to disparate contributions from one of the
most diverse committees I have ever served on. (I think that both the
lawyers and the philosophers outnumbered the three "computerists" on the
committee--it was a very broadening experience.)

I must confess that I am now much less confident that much privacy can be
salvaged than I was when the study was started.

<<http://virtualbumperstickers.blogspot.com/2006/05/you-have-zero-privacyanywayget-over-it.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

Search RISKS using [swish-e](#)

Volume 24: Issue 69

Thursday 14 June 2007

Contents

- [Hurricane forecasting uncertainty](#)
[Jessica Gresko PGN-ed](#)
- [Glitch Blamed for Fire Alarm on Orbiter](#)
[John Schwartz PGN-ed](#)
- [Casting Ballot From Abroad Is No Sure Bet](#)
[Ian Urbina PGN-ed](#)
- [Lawsuits mounting over massive customer data breach at TJX](#)
[Mark Jewell via Monty Solomon](#)
- [Hotel wake-up calls and daylight savings deja vu](#)
[Kevin Fu](#)
- [Council builds database of burglary targets](#)
[Adam Laurie](#)
- [Man risks five years jail time for using open WiFi connection](#)
[Nick Brown](#)
- [Urgent Call For a Google At-Large Public Ombudsman](#)
[Lauren Weinstein](#)
- [AT&T's Internet Monitoring Plans](#)
[Lauren Weinstein](#)

- [Just a few clicks sends all pupils NSFW pictures](#)
[Debora Weber-Wulff](#)
 - [Risks of secure e-mail access](#)
[Nick Brown](#)
 - [Bloat: 1986 personal computer outperforms 2007 personal computer](#)
[Daniel P. B. Smith](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Hurricane forecasting uncertainty

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

Thu, 14 Jun 2007 10:07:17 PDT

The National Oceanic and Atmospheric Administration chief has said written that the anticipated failure of QuikScat ("an aging weather satellite crucial to accurate predictions on the intensity and path of hurricanes", launched in 1999 and designed to last only a few years) could add uncertainty to forecasts and broaden the areas over which hurricane warnings and watches would have to be invoked. (The estimated cost of evacuations is about \$1 million per mile of coastline.) Accuracy of predictions has doubled in the past 15 years, but would be set back by delays and lack of funding for the desired replacement -- which might require four years and \$400 million. (QuikScat suffered a transmitter failure in 2006, and has been using a backup transmitter.) Source: Jessica Gresko, AP item, seen in the **San Francisco Chronicle**, 14 Jun 2007, A17; PGN-ed]

✶ Glitch Blamed for Fire Alarm on Orbiter

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

Wed, 13 Jun 2007 14:17:11 PDT

After the failure of the computer control systems in the Russian part of the International Space Station and the subsequent inability of the Russian computers to work with the American computers, control was reportedly passed to maneuvering jets on the Atlantis shuttle. The Space Station solar panel configuration was unable to generate enough power, and certain functions had to be shut down manually -- which caused the software to trigger a fire alarm in the Russian part of the Space Station. It took twenty minutes to diagnose that it was a false alarm, and that there was no fire. [Source: John Schwartz, *The New York Times*, 13 Jun 2007; PGN-ed]

✶ Casting Ballot From Abroad Is No Sure Bet

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

Wed, 13 Jun 2007 14:03:48 PDT

Voting over the Internet is a topic that has often appeared in RISKS: in general ([RISKS-21.15](#) and many more issues), and particularly relating to the U.S. (SERVE), the Netherlands, the Philippines, Switzerland, and so on.

Today's NYTimes article notes that the U.S. DoD has expended

over \$30 million seeking to enable U.S. military and civilians to vote dependably, with no viable solution yet in hand. The article notes that the existing Web-based system is slow and confusing, with many security and privacy problems. It was used by only 63 military voters in the November 2006 election. Civilians are not able to use it. Absence of standards among different states is problematic. Many overseas voters have been unable to cast votes. [Source: Ian Urbina, New York Times, 13 Jun 2007; PGN-ed]

<http://www.nytimes.com/2007/06/13/washington/13overseas.html>

[As noted in previous RISKS issues, voting by Internet is inherently riskful, particularly with respect to voter coercion, vote selling, tampering, denials of service, and other problems. PGN]

⚡ Lawsuits mounting over massive customer data breach at TJX

<Monty Solomon <monty@roscom.com>>

Wed, 13 Jun 2007 20:48:13 -0400

Since the 28 Mar 2007 filing that listed over a dozen lawsuits, the TJX Cos. Inc. now faces nine more federal lawsuits in five additional states over the data theft that exposed at least 45 million credit and debit cards to potential fraud. Fifth Third Bancorp is also named. [Source: Mark Jewell, Associated Press, 8 Jun 2007; PGN-ed]

<http://www.metrowestdailynews.com/business/x1289425994>

✈ Hotel wake-up calls and daylight savings deja vu

<Kevin Fu <kevinfu@cs.umass.edu>>

Fri, 1 Jun 2007 12:39:05 -0400

Daylight savings time produced some annoyances earlier this year, but on 1 Apr 2007 it produced some unexpected personal inconveniences. My hotel's wake-up call system malfunctioned because it "double counted" daylight savings time. I suspect that the hotel manually pushed time forward earlier in the year, but forgot to disable the automated daylight savings time event that previously took place on the first Sunday in April at 2AM. That would be April Fool's Day 2007. My wake-up call was set to 4:30AM, but actually rang at 3:30AM. After attempting to re-set the wake-up call for 4:30AM (which, of course, was futile since it would ring the next day), I slept through my flight home and had to buy a new ticket. The daylight savings deja vu added a redevye to my travel, and my lecture the next morning was probably quite loopy.

Anyhow, I'm surprised there was not much discussion on what would happen on the historical day of daylight savings. Most discussion focused on what would happen on the new day of daylight savings. That's simple: People manually set their clocks trying to outsmart software. There will probably be similar "double daylight" problems in the Fall on the

historical dates
for daylight savings for years to come.

The "smart" wall clocks in the hotel's fitness center also set themselves forward twice, now an hour ahead of correct time. Pictures on <http://kevinfu.blogspot.com/>. Can you guess the hotel?

Kevin Fu, Assistant Professor, Computer Science Department,
University of
Massachusetts Amherst 1-413-545-4006 <http://www.cs.umass.edu/~kevinfu/>

[Ah, yes, recall Caltrain's double daylight time ([RISKS-24.63](#)). PGN]

⚡ Council builds database of burglary targets

<Adam Laurie <adam.laurie@thebunker.net>>
Wed, 06 Jun 2007 12:39:22 +0100

Yesterday, while working at home, I received a visit from someone purporting to be from my local council, and he had an ID badge to prove it. He also had a copy of a letter which I should have received, and a fairly comprehensive survey form for the activity he wished me to participate in. In brief, it was a survey of "Housing Conditions", based on a randomly selected number of houses, and intended to allow the council to extrapolate the overall condition of the houses in their area for grant funding planning purposes. All fine so far, but now onto the questionnaire that goes with the survey...

As well as the obvious stuff about the condition of the property, there was also an extensive "Socio-Economic" section. This attempted to determine the net worth of the individuals in the property, as well as original cost, value of contents etc. This was worrying enough in itself, but the final straw was in a section they called "Health and Safety", which included an item called "3rd Party Intrusion Risk". This was basically a breakdown of how easy (and therefore likely) it was to break in to the building, and details of any specific weaknesses. At this point alarm bells were ringing loudly and I started to question who would have access to this data.

I was given the usual platitudes:

"The data won't be linked to any specific building."
(So why is the address written on the front of the form?)

"Only this department will use the data and only for a specific planning purpose."
(At this point it turned out he doesn't work for the council at all, but is working for a firm sub-contracted to do this work nationwide. Who've just been bought.)

"All staff are vetted."
(Don't get me started on local government vetting. Oh, but wait, he now works for company B, who bought company A, who does the work for the council, so couldn't even tell me who the staff were or where the data entry team were based).

"Nobody but us would understand it."

(Errr... Yeah, right.)

"The intrusion risk questions are to do with mental health."
(??? Apart from being utterly confusing, that's also utterly irrelevant.

Mr. Burglar is not going to care *why* you collated this useful tidbit for him, only that you did!)

etc.

I think the risks of collating a database of houses, the wealth of the owner, the value of the contents and a handy scale of difficulty of entry complete with tips on where to look are manifest, particularly given the ongoing revelations about "data loss" from similar organisations...

I, for one, declined to participate. :)

Adam Laurie, The Bunker Secure Hosting Ltd., Ash Radar Station,
Marshborough
Road, Sandwich, Kent CT13 0PL, UNITED KINGDOM +44 (0) 1304 814800

[This may sound familiar, but is certainly worth a RISKS warning. I am

reminded of a would-be burglar-alarm company that operated for a while in

Watchung NJ (near Bell Labs), giving free detailed house security

assessments and alarm-system estimates. Somewhat later, the most

opportune of those homes that did NOT subscribe to the alarm system were

burgled, within a short period of time, after which the perpetrators

vanished. PGN]

✦ Man risks five years jail time for using open WiFi connection

<"Nick Brown" <Nick.BROWN@coe.int>>

Fri, 25 May 2007 10:54:58 +0200

A Michigan man who was caught using a coffee shop's unsecured WiFi connection while sitting in the car park was fined \$400 and ordered to do 40 hours community service. But he could have received a 5-year jail term, as the state law which covers this is part of a 1979 anti-hacking bill which makes this a felony.

http://news.com.com/8301-10784_3-9722006-7.html

I suspect he needs a better lawyer. If the coffee shop wants to limit access to customers, it can do so easily by issuing (free) username/password tickets and having the proxy server require a valid logon to connect. Indeed, in many cases where multiple WiFi networks are available, it is not possible to know where each is situated and which don't mind if you use them without any other form of purchase.

In this case, the coffee shop owner did not complain; the man was spotted by a law enforcement officer who asked him what he was doing and then had to check that it was actually illegal. Again, I wonder what a better lawyer would have made of this, which seems - at first sight to this non-lawyer - to constitute self-incrimination.

🚨 Urgent Call For a Google At-Large Public Ombudsman

<Lauren Weinstein <pfir@pfir.org>>

Mon, 11 Jun 2007 08:17:57 -0700 (PDT)

Urgent Call For a Google At-Large Public Ombudsman

<http://lauren.vortex.com/archive/000251.html>

June 11, 2007

In both public and government circles, concerns are rising regarding important aspects of Google's ongoing operations. Some of these concerns are very real, and some are more a matter of perception than reality -- often magnified simply because Google is involved. In either case, the situation is exacerbated by the extremely limited opportunities for the public to interact directly with Google in a meaningful way regarding increasingly sensitive matters that can have highly personal and very widespread impacts.

A dedicated, at-large, public ombudsman to deal with these issues is urgently needed at Google, to interact directly and routinely with the public regarding Google, YouTube, and other affiliated operations.

The privacy, content-related, and many other concerns of ordinary users and organizations, expressed to Google through currently available feedback channels, appear to routinely vanish into what is effectively a "black hole" -- with a lack of substantive responses in most cases. If you don't have a court order or a DMCA "take down" notice, Google can appear

impenetrable to
expressed concerns.

Privacy International's reported inability to receive a response to their queries prior to the release of a new report regarding Google privacy is but one example of a seemingly pervasive situation at Google (<http://www.cnbc.com/id/19153743>).

I won't present here a critique of that report itself, but it's clear that both individuals and organizations commonly feel impotent when attempting to resolve many important issues with Google directly.

In general, both politicians and government agencies appear increasingly unsatisfied with this status quo, and their reactions could be extremely damaging to Google and the broader Internet.

I'm not suggesting another Google counsel. The ombudsman would have a role wholly different from that of Peter Fleischer's Global Privacy Counsel position, or Nicole Wong's Deputy General Counsel role. In fact, this would likely not primarily be a policy "development" role per se, though policy evolution over time would of course be significantly involved.

The ombudsman would be a non-lawyer who would be assigned full-time to act as an easily approachable and highly available front-line interface between the public and Google operational/R&D teams. This individual would be the primary initial contact for most queries from individuals and organizations who have specific problems related to Google content, privacy, or a range of other related policy matters. This technically knowledgeable individual

would be well-versed regarding the relevant issues and ideally already possess a high degree of trust within the larger Internet community.

Such an ombudsman, by fostering open lines of communications, could immediately interact with members of the public and push relevant matters quickly up the chain of command inside Google for action as appropriate.

There's simply no legitimate excuse for a public communications void of such a magnitude at this stage of Google's development, especially with an organization of Google's size, market share, influence, and immense technical competence. At a minimum, ordinary Google users should be able to get quick, reliable, and substantive responses and resolving dialogue for their Google-related concerns, even irrespective of any final dispositions.

Communication is incredibly important in this sphere. The current situation is seriously and increasingly dangerous to Google. Backlash and reactive, knee-jerk legislation by ambitious politicians could easily unreasonably constrain and seriously damage Google, the broader Internet, and Net users around the world.

A Google at-large ombudsman along the lines that I've outlined could be the best and most practical way to help avoid such negative outcomes, while not disrupting Google's operations and growth. It would most decidedly not be an easy job for anyone, but would be an important position that definitely

needs to exist.

I make this recommendation with what I believe are the best interests of both Google and the Net's users in mind. I want to see Google continue in its success. But a regulatory and public relations train wreck -- with major collateral damage across the Internet -- is increasingly likely unless serious and comprehensive improvements in Google's handling of this area are forthcoming in the extremely near future.

The appointment of a qualified and dedicated ombudsman, with the sincere support and confidence of Google high-level management, could go a long way toward making Google an acknowledged leader in responsive operations, to the benefit of us all.

Of course, it's not impossible that this call for a Google ombudsman will itself be ignored by Google. But in the final analysis, we can all hope that Google management will realize that creating this position is very simply the right thing to do.

Lauren Weinstein <http://www.pfir.org/lauren> +1(818) 225-2800
lauren@pfir.org
Co-Founder, PFIR: People For Internet Responsibility - <http://www.pfir.org>
PRIVACY Forum - <http://www.vortex.com> Lauren's Blog: <http://lauren.vortex.com>

AT&T's Internet Monitoring Plans

<Lauren Weinstein <lauren@vortex.com>>

Thu, 14 Jun 2007 07:50:54 -0700

AT&T's Internet Monitoring Plans

<http://lauren.vortex.com/archive/000252.html>

News stories are now appearing widely about an AT&T plan to try block

pirated content *at the network level*. See this example from the Los

Angeles Times:

<http://www.latimes.com/business/la-fi-piracy13jun13,1,2155771.story>

The implications of this sort of network snooping are immense.

One might

assume that a primary target will be file sharing technologies.

But to

actually pick out particular content from those streams would imply the need

to actually examine and characterize the payload of files to locate and

block potentially offending music and/or video content.

AT&T will no doubt suggest that this activity is akin to virus and spam

filtering of e-mail for their customers. This would be a specious analogy.

Spam filtering can usually be controlled by the user, and virtually all AT&T

mail processing can be avoided by their customers if AT&T servers are not

used.

However, it sounds as if AT&T is planning a network monitoring regime that

would not be dependent on the use of AT&T servers. What's more, the

"benefits" of this monitoring would not be directed to the customers whose

traffic is being monitored, but rather for the benefit of unrelated third

parties.

"Fingerprinting" of content for anti-piracy purposes is not always unacceptable. For example, Google/YouTube is reportedly starting tests of a copyrighted material characterization blocking system. Since users submitting videos to YouTube are doing so with the expectation of that content being hosted there, it is not unreasonable for YouTube to avoid hosting pirated materials whenever practicable.

However, AT&T's proper role in this context (among an ever smaller number of ISP choices) is simply to move customer data traffic between points, not to be a content policing agent for third-party commercial interests, or a mass data conduit for government interests without appropriate legal authority, for that matter. The traffic under discussion, based on news reports about the AT&T plans so far, would typically not be directed to AT&T servers, and should not be subject to content inspection by AT&T, in the absence of specific targeted court orders or the like.

We can get into a discussion of if and how common carrier considerations play into any of this anymore, and how encryption (and attempts to control and suppress encryption) will enter the mix, but the very fact that these AT&T plans have gotten this far is extremely disturbing.

Finally, perhaps the most illuminating aspect of this situation is a statement by James W. Cicconi, an AT&T senior vice president, who is quoted as saying that AT&T wouldn't look at the privacy and other legal

issues

involved until **after** a monitoring technology has been chosen.

That pretty much says it all.

Lauren Weinstein <http://www.pfir.org/lauren> +1(818) 225-2800

lauren@pfir.org

PRIVACY Forum - <http://www.vortex.com> Lauren's Blog: <http://lauren.vortex.com>

⚡ Just a few clicks sends all pupils NSFW pictures

<Debora Weber-Wulff <D.Weber-Wulff@fhtw-berlin.de>>

Sun, 10 Jun 2007 16:25:32 +0200

The Swedish newspaper Sydsvenskan reports (June 6, 2007) on a problem

that affected some 10.000 pupils in the Lund school district:

<http://sydsvenskan.se/lund/article243800.ece>

It seems that whoever set up the mailing lists thought it would be a nice

idea if one could send an e-mail to every pupil at once, perhaps to announce

snow days or whatever. However, this function was open to everyone.

A pupil obtained some NSFW material and decided to send it on to all of

his fellow pupils. An administrator is quoted describing the material:

"Det är så grovt att det inte kan uttryckas i ord. Jag har aldrig sett

något vidrigare." (I cannot describe the brutality in words. I have

never seen anything this disgusting before.)

It took a number of days to remove the material from the servers after the incident came to light. The server was rented in another country (Norway) and it apparently took some convincing for them to go in and remove all copies of this e-mail, as there were so very many accounts affected. [Each account probably had to be looked at by a human. -dww]

The school administration is debating whether to file charges against the pupil [I would instead file the charges against the person setting up this nonsense - dww], and has disabled the mass mailing functionality.

Prof. Dr. Debora Weber-Wulff, FHTW Berlin, Treskowallee 8, 10313 Berlin
+49-30-5019-2320 <http://www.f4.fhtw-berlin.de/people/weberwu/>

✦ Risks of secure e-mail access

<"Nick Brown" <Nick.BROWN@coe.int>>
Fri, 1 Jun 2007 12:51:56 +0200

At our site, we use a number of techniques to detect malware infestation on our Windows XP-based PCs. One of these is the monitoring of auto-run locations in the Windows registry, because most malware installs itself to run automatically at system startup or logon time.

The other day our system called out a piece of auto-running software in the user account of a visitor to our site, who was on loan to us for a week from a UK government institution. I assumed it was yet another minor

piece of
drive-by malware from a Web site, took our usual first-level
action (remove
registry entry, delete software) and assumed that would be that.

Next day, the software was back. I took a closer look. It had
installed a
directory called "Whale Communications" in the "Program Files"
directory,
containing a .EXE file and numerous DLLs. I carefully checked
the registry
of the PC, re-deleted the software (this required killing
Internet Explorer
on the PC), and waited. Within an hour, it was back.

Now, when we get to this point, one of two things is usually
going on;
either the user is hitting a particular porn/warez/game site
very hard, or
the malware uses some fairly classy techniques to keep itself
installed. So
I disabled the user's account, rebooted the PC, and waited for
the phone to
ring.

Well, it turns out that all he was doing was reading his home
office e-mail.
His organisation uses a "key-ring" code generator gadget which
requires code
to be running on the client PC. So their remote e-mail portal
detects
whether this code is present, and if not, the browser
automagically
downloads it to the PC and installs it to auto-run.

Slightly shocked at the rudeness (not to mention unreliability)
of this
approach, I called the organisation's IT department. My
suggestion that it
might not be a good idea to work this way was greeted with very
little
comprehension. Apparently, their in-house culture is that
anyone is allowed

to download anything they like, and nobody had given much thought to whether different rules might apply elsewhere (at our site, we can potentially have people physically removed from the building in such cases).

I pointed out that there are plenty of challenge-response solutions out there which are entirely Web-based and don't require what, in many jurisdictions, would be regarded as vandalism or hacking of the PC being used, but the response was "well, this is the first time we've heard about this problem". (Regular RISKS readers may have heard that one before.)

So the risks are multiple, ranging from being unable to get to your e-mail from any Internet cafe' as promised, if said Internet cafe' runs an OS for which the client software isn't available and/or has download blocking in operation, through to potential expulsion from the country or imprisonment (I don't like to think what might have happened had the person in question been using a computer in a US federal government office or one in several countries which I could name).

🔥 Bloat: 1986 personal computer outperforms 2007 personal computer

<"Daniel P. B. Smith" <dpbsmith@verizon.net>>
Sun, 03 Jun 2007 11:26:03 -0400

Re the thread on touch typing, and Martin Ward's quotation:

"The most amazing achievement of the computer software industry is its continuing cancellation of the steady and staggering gains made by the computer hardware industry..."-- Henry Petroski

A recent discussion in Slashdot referenced an article by Hal Licino: Licino compared a 1986 Mac Plus with 4 meg of RAM, and 8MHz 68000 and a 40MB hard drive running Mac OS 6.0.8, to a 2007 AMD Athlon 64 X2 4800+ with 1GB of RAM, two 2.4GHz processors, and a 120 GB hard drive running Windows XP Professional SP2. He carefully details the test conditions and the rationale for the system configurations he chose.

<http://hubpages.com/hub/>

[86 Mac Plus Vs 07 AMD DualCore You Wont Believe Who Wins](#)

The tests basically tested only two applications, Microsoft Word and Microsoft Excel, and it seems to me that the things he chose to measure were very reasonable, and not unrepresentative of ordinary use.

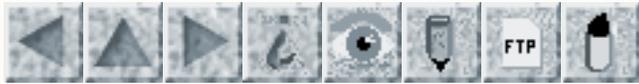
The 1986 computer won 9 out of 17 of his tests.

RISKS readers can read his article and decide what quibbles they have with the results.

But the point is made. It is as if someone were to find that it took a roughly comparable time fly from Albany to Buffalo today as it took to travel on the Erie Canal.

(For the record, the fastest and slowest itineraries Travelocity shows me for this 289-mile trip, are 1 hr. 10 minutes for a nonstop flight, and 5 hrs

57 min for an itinerary changing planes in Detroit. The average speed of 48 mph for that second option gives one pause, but it is still twenty-four times as fast as the fastest packets on the Erie Canal, which took 6 days.)



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 70

Tuesday 19 June 2007

Contents

- [Gripen: Risks of safety measures in military jet aircraft](#)
[Tony Lima](#)
- [EFF: Court Protects Email from Secret Government Searches](#)
[Kevin Bankston via David Farber](#)
- [Blogger unmasked, court case upended](#)
[Jonathan Saltzman via Monty Solomon](#)
- ["Deleted" children in Japan](#)
[Rodney Van Meter via Dave Farber](#)
- [More on the Space Station problem](#)
[PGN](#)
- [Improving reliability of health critical software](#)
[Marc Auslander](#)
- [Search Engine Dispute Notifications: Request For Comments](#)
[Lauren Weinstein](#)
- [Extending Google Blacklists for Dispute Resolutions](#)
[Lauren Weinstein](#)
- [Re: USAF F-22 jets grounded by software glitch](#)
[Gregory Chapelle](#)

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

Gripen: Risks of safety measures in military jet aircraft

<Tony Lima <tony.lima@csueastbay.edu>>

Tue, 29 May 2007 17:25:12 -0700

Swede's Perfect Spontaneous Ejection, 29 May 2007

<http://www.strategypage.com/htmw/htmurph/articles/20070529.aspx>

Last month, a Swedish Gripen fighter crashed when the pilot suddenly ejected. The pilot insisted that he had not activated the ejection system. After intense investigation, and lots of computer simulation of flight systems, investigators concluded that the pilots account of events was accurate. Turns out that if enough g-force is applied to the aircraft, the pilot ejection system automatically activates. This leaves the aircraft without a pilot, right after it has performed a stressful maneuver (to produce the high g-force.)

This sort of thing is increasingly common with modern weapons systems. That because these systems are increasingly more complex systems of systems, where it has become impossible to forecast all of the possible unpleasant, and unwanted, events that could occur under certain situations.

Tony Lima, Professor of Economics, California State University, East Bay
Hayward, CA 94542 1-510-885-3889 <http://www.cbe.csueastbay.edu/~alima>

[Gripen grep'n grabs gripin':

[RISKS-8.32](#),49, 14.81,82,85, 15.04,19,25,26. PGN)

EFF: Court Protects Email from Secret Government Searches

<David Farber <dave@farber.net>>

Mon, 18 Jun 2007 17:33:04 -0400

Electronic Frontier Foundation Media Release, Monday, June 18, 2007

Contact: Kevin Bankston, Staff Attorney, Electronic Frontier Foundation

bankston@eff.org, +1 415 436-9333 x126

Court Protects Email from Secret Government Searches

Landmark Ruling Gives Email Same Constitutional Protections as Phone Calls

San Francisco - The government must have a search warrant before it can

secretly seize and search emails stored by email service providers,

according to a landmark ruling Monday in the 6th U.S. Circuit Court of

Appeals. The court found that email users have the same reasonable

expectation of privacy in their stored email as they do in their telephone

calls -- the first circuit court ever to make that finding.

Over the last 20 years, the government has routinely used the federal Stored

Communications Act (SCA) to secretly obtain stored email from email service

providers without a warrant. But today's ruling -- closely following the

reasoning in an amicus brief filed the by the Electronic

Frontier Foundation

(EFF) and other civil liberties groups -- found that the SCA violates the Fourth Amendment.

"Email users expect that their Hotmail and Gmail inboxes are just as private as their postal mail and their telephone calls," said EFF Staff Attorney Kevin Bankston. "The government tried to get around this common-sense conclusion, but the Constitution applies online as well as offline, as the court correctly found. That means that the government can't secretly seize your emails without a warrant."

Warshak v. United States was brought in the Southern District of Ohio federal court by Steven Warshak to stop the government's repeated secret searches and seizures of his stored email using the SCA. The district court ruled that the government cannot use the SCA to obtain stored email without a warrant or prior notice to the email account holder, but the government appealed that ruling to the 6th Circuit. EFF served as an amicus in the case, joined by the American Civil Liberties Union and the Center for Democracy & Technology. Law professors Susan Freiwald and Patricia Bellia also submitted an amicus brief, and the case was successfully argued at the 6th Circuit by Warshak's counsel Martin Weinberg.

For the full ruling in Warshak v. United States:

http://eff.org/legal/cases/warshak_v_usa/6th_circuit_decision_upholding_injunction.pdf

For EFF's resources on the case, including its amicus brief:

http://www.eff.org/legal/cases/warshak_v_usa/

For this release:

http://www.eff.org/news/archives/2007_06.php#005321

About EFF: The Electronic Frontier Foundation is the leading civil liberties organization working to protect rights in the digital world. Founded in 1990, EFF actively encourages and challenges industry and government to support free expression and privacy online. EFF is a member-supported organization and maintains one of the most linked-to websites in the world at <http://www.eff.org/>

[Whereas this is an appealing ruling to privacy advocates, it seems likely to be appealed. PGN]

⚡ Blogger unmasked, court case upended (Jonathan Saltzman)

<Monty Solomon <monty@roscom.com>>

Sat, 2 Jun 2007 00:17:19 -0400

Pediatrician Robert P. Lindeman was defending himself in a malpractice suit involving the death of a 12-year-old patient, in Massachusetts Suffolk Superior Court. The opposing counsel asked him whether he was the blogger ("Flea") who had been writing about a trial that sounded very similar, ridiculing the plaintiff's case and the lawyer, revealing the defense's strategy, and accusing members of the jury of "dozing". Lindeman admitted he was indeed Flea. He then wound up paying a "substantial settlement" and

the case was closed. [Source: Jonathan Saltzman <jsaltzman@globe.com>, *The Boston Globe*, 31 May 2007; PGN-ed. No one seems to have noticed various opportunities for puns: Lindeman was copping a flea and fleaing the coup.]

http://www.boston.com/news/local/articles/2007/05/31/blogger_unmasked_court_case_upended/

✦ "Deleted" children in Japan (via Dave Farber's IP)

<Rodney Van Meter <rdv@sfc.wide.ad.jp>>

May 30, 2007 10:44:22 PM EDT

This tidbit bothers me because it speaks to the entire future of our history in the world in which "If Google can't find it, it doesn't exist."

A little background: in Japan, you don't have a birth certificate. Each family has a family registry, and children who are born are entered into the registry. I think the same holds for proof of marriage. Generally, the registry has a family name on it (just one -- making it difficult for women to keep their maiden names, but that's not the point here) and a head of household. Then underneath that are the members of the household -- wife and kids. Normally, kids stay on their parents' registry until they marry or the parents die. When you marry, you move off your parents' registry and start your own. You do your registration at the city office, but it's a national registry run by the Justice Department.

In the normal progress of things, of course, the last entry for each child is a notation that they moved off of this registry and onto another one. But if a child dies, then a notation is made of that fact.

An article in yesterday's Daily Yomiuri <http://www.yomiuri.co.jp/dy/features/culture/20070530TDY02009.htm> says that they are still in the process of digitizing the registry, and that some deceased children are being "deleted" in the process, simply to keep down the amount of data input work (which undoubtedly has to be done by hand).

While it certainly makes sense to prioritize the digitization of currently-active families, as opposed to the historical records of deceased grandparents whose registers consist of no one alive, this choice has the effect of creating an apparently complete registry of an active family that portrays an inaccurate picture of the family history.

From the article:

According to the [Justice] ministry, the names of family members who died before the digitization have been included on the original hard copy of the family registry as one who has been "removed." But the names, the ministry said, have been stricken from the data files.

The reasoning behind this was an attempt to reduce the data input into the system--by even only a bit--during the digitization process. Family members who died following the move of data files are still represented in the electronic registers.

"You've got it backward if you think digitizing family registers will result in more work," a ministry official said. "Even if the name of the deceased disappears from the data, you can still see it on the original, so it isn't a problem."

"isn't a problem"! A hundred years from now no one will know that the families in question ever **had** children. Looking at a particular digital record, you wouldn't even know to **ask** to see the original hard copy. Statistics on births and deaths from various causes will no doubt be skewed, let alone the impact on genealogy.

While it seems likely that eventually they will get around to digitizing historical records, this particular gap in the data seems unlikely to be fixed -- or even fixABLE, without a second by-hand check of every registry comparing the original hard copy with the digitized version.

There are gaps in my family history where, e.g., the courthouse holding birth certificates burned down. But at least we **know** that there are gaps.

Is this a bigger loss than, oh, say, the burning of the library at Alexandria, or the one at Bukhara (~650 and again 1920), or the burning of Mayan texts by the Spanish? Nah. But I mourn the loss of every bit(!) of our collective history.

IP Archives: <http://v2.listbox.com/member/archive/>

✦ More on the Space Station problem (Re: [RISKS-24.69](#))

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

Tues, 19 Jun 2007 10:10:53 PDT

Re: Glitch Blamed for Fire Alarm on Orbiter ([RISKS-24.69](#))

The problem on the Space Station turned out to be a faulty switch. Each of two sets of computers has three redundant channels ("lanes"), at least one of which must work for each system. All six lanes crashed and could not be restarted. The patch involved hooking up jumper cables and managing to get at least two pairs of lanes working again. This is considered a temporary fix, with astronauts working externally to "isolate the computers from connections with newly deployed solar panels that may have set off the problem." [Source: John Schwartz, *The New York Times*, 16 Jun 2007, National Edition A8; PGN-ed]

Beginning after the installation of a 17.2-ton truss a week ago, crashes disrupted the Russian computers that control environmental systems and the thrusters that regulate the Space Station's orientation. Over the weekend, Russian astronauts isolated the problem to the surge protector circuitry, which they were able to bypass. Systems are once again working -- although the original cause is still unknown and being sought. [Source: Kenneth Chang, *The New York Times*, 19 Jun 2007, National Edition A14; PGN-ed]

✦ Improving reliability of health critical software

<"Marc Auslander" <marcausl@optonline.net>>

Thu, 14 Jun 2007 19:08:26 -0400

(Re: Cook, FDA recall, [RISKS-24.68](#))

The article about a faulty algorithm in a laser eye surgery unit (Alcon Refractive Horizons and FDA notified healthcare professionals and patients of a Class I Recall...) got me wondering about how to reduce the chances of such disasters. It seems to me that the technique of redundant independent implementations might be useful. We all know the idea - give the specs to two (or more groups) and get software from each. In operation, run all the versions, compare the results, and do something special if they mismatch.

The space shuttle software has used this technique for quite a while. It lead to one famous mission scrub because of a problem with the comparison logic, but that's OK. And in cases like the above, you should be able to do the check before you commit to the procedure, so the special thing you do is to stop.

✦ Search Engine Dispute Notifications: Request For Comments

<Lauren Weinstein <lauren@vortex.com>>

Fri, 15 Jun 2007 13:33:46 -0700

Search Engine Dispute Notifications: Request For
Comments

<http://lauren.vortex.com/archive/000253.html>

Greetings. I'd appreciate feedback from the Internet community regarding the following issue.

Search engines have of course become the primary means by which vast numbers of people find all manner of information. For many firms, if you don't have a high rank with Google, it's as if you don't exist (or at least, many companies appear to feel that way).

Increasingly, cases are appearing of individuals and organizations being defamed or otherwise personally damaged -- lives sometimes utterly disrupted -- by purpose-built, falsified Web pages, frequently located in distant jurisdictions. Search engine results are typically the primary means by which such attacks are promulgated and sustained by providing a continuing stream of viewers to those Web pages. Due to ranking algorithms, attempts to counter such attacks with other Web pages may not be widely seen since they are not directly associated with the attacking pages.

Courts appear generally reluctant to order offending Web page take downs in such cases, except where intellectual property (e.g. DMCA orders) are involved, and take downs do not necessarily inform viewers of the ongoing controversy in a logically connected manner. Additionally, "remedies" that

result in suppression of information, rather than providing additional information, are generally ineffective and counter to the "open information whenever possible" philosophy that many of us share.

Question: Would it make sense for search engines, only in carefully limited, delineated, and serious situations, to provide on some search results a "Disputed Page" link to information explaining the dispute in detail, as an available middle ground between complete non-action and total page take downs?

Search engine firms have generally taken the view that they are akin to telephone directories, and bear no responsibility for the content of the pages that they reference. Similarly, when ostensibly aggrieved parties approach these firms with concerns about "offending" pages, the usual response is that the search firms can do nothing about those pages, and that any complaints need to be taken to the Web page owner or associated ISP. From a practical and jurisdictional standpoint, this turns out to be impossible in many cases.

We clearly do not want to hold search engines responsible for other sites' content, even when locally cached. To do so would likely obliterate the entire search engine model and industry under a storm of litigation, to everyone's detriment. It must be noted, however, that increasing calls for holding search engines responsible in just such a manner are being heard in some political and judicial circles, likely out of frustration

with the status quo, which currently tends not to offer reasonable dispute resolution paths in most situations. This is a serious warning sign, suggesting that we should consider some new approaches on our own, or risk draconian and damaging legislation.

The telephone directory argument also has some problems. Unlike typical phone books, search engines are not passive publishers of information. In addition to third-party ads tied to the core listings, a key facet of search engines is intensive ranking and decision-based ordering of content listings, usually via highly proprietary algorithms. Such ranking provides a high percentage of the value-added represented by search engine results.

So while search engines are not responsible and should not be held responsible for the content of the outside pages and data they index, they are very much directly involved as decision-making gatekeepers (albeit, usually through fully automated algorithms) that determine to a major extent which individual Web pages are likely -- or unlikely -- to be discovered by Internet users.

More questions: Given the power that search engines possess in these regards, do they bear any responsibility for helping to untangle serious disputes regarding the pages they reference and often profit from? If search engines do not voluntarily move in this direction, do they risk damaging legislation written without a genuine understanding of

the complex
technical and business issues involved?

In my view, an evolution by search engines to deal with these situations should be predicated on that key concept of maximizing the availability of information. Page take downs -- which are likely to be ineffective in the long run as noted -- should be a last resort.

Similarly, a total laissez faire approach is also unlikely to be tolerated indefinitely by the political and judicial establishments.

So returning to where we started... Could some sort of "dispute link" -- tied directly to information regarding particularly serious page disputes -- provide a reasonable means to help ameliorate these situations without risking the more destructive alternatives? If so, how would such a system be effectively implemented in a practical fashion? How could such a system be structured to avoid being swamped by relatively trivial complaints?

Would providing related dispute links only to persons with court orders make sense to limit potential abuse of the mechanism, or would requiring the use of the expensive and delay-prone courts be far too restrictive a qualification? Could such a dispute system operate purely on a voluntary basis? (Voluntary would be very much preferred in my opinion.) What are the cost factors involved in such a system and how could they be reasonably addressed?

Overall then, is it possible to structure such a system along these lines so that it is practical, workable, and also palatable to the major

search

engine firms, as an alternative to barreling along toward an onerous and likely politically motivated crackdown down the line?

Or would this concept just never work -- and that crackdown is inevitable?

Your thoughts would be appreciated. Thanks very much.

Lauren Weinstein <http://www.pfir.org/lauren> +1(818) 225-2800
lauren@pfir.org

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

PRIVACY Forum - <http://www.vortex.com> Lauren's Blog: <http://lauren.vortex.com>

✶ Extending Google Blacklists for Dispute Resolutions

<Lauren Weinstein <lauren@vortex.com>>

Sun, 17 Jun 2007 16:56:45 -0700

Extending Google Blacklists for Dispute Resolutions
<http://lauren.vortex.com/archive/000254.html>

Greetings. In (<http://lauren.vortex.com/archive/000253.html>) I discussed some issues regarding search engine dispute resolution, and posed some questions about the possibility of "dispute links" being displayed with search results to indicate serious disputes regarding the accuracy of particular pages, especially in cases of court-determined defamation and the like.

While many people appear to support this concept in principle,

the potential operational logistics are of significant concern. As I originally acknowledged, it's a complex and tough area, but that doesn't make it impossible to deal with successfully either.

Some others respondents have taken the view that search engines should never make "value judgments" about the content of sites, other than that done (which is substantial) for result ranking purposes.

What many folks may not realize is that in the case of Google at least, such more in-depth judgments are already being made, and it would not necessarily be a large leap to extend them toward addressing the dispute resolution issues I've been discussing.

Google already puts a special tag on sites in their results which Google believes contain damaging code ("malware") that could disrupt user computers. Such sites are tagged with a notice that "This website may damage your computer." -- and the associated link is not made active (that is, you must enter it manually or copy/paste to access that site -- you cannot just click).

Also, in conjunction with Google Toolbar and Firefox 2, Google collects user feedback about suspected phishing sites, and can display warnings to users when they are about to access potentially dangerous sites on these lists.

In both of these cases, Google is making a complex value judgment concerning the veracity of the sites and listings in question, so it

appears that this horse has already left the barn -- Google apparently does not assert that it is merely a neutral organizer of information in these respects.

So, a site can be tagged by Google as potentially dangerous because it contains suspected malware, or because it has been reported by the community to be an apparent phishing site. It seems reasonable then for a site that has been determined (by a court or other agreed-upon means) to be containing defaming or otherwise seriously disputed information, to also be potentially subject to similar tagging (e.g. with a "dispute link").

Pages that contain significant, purposely false information, designed to ruin people's reputations or cause other major harm, can be just as dangerous as phishing or malware sites. They may not be directly damaging to people's computers, but they can certainly be damaging to people's lives. And presumably we care about people at least as much as computers, right?

So I would assert that the jump to a Google "dispute links" mechanism is nowhere near as big a leap from existing search engine results as it may first appear to be.

In future discussion on this topic, I'll get into more details of specific methodologies that could be applicable to the implementation of such a dispute handling system, based both within the traditional legal structure and through more of a "Web 2.0" community-based topology.

But I wanted to note now that while such a search engine dispute

resolution
environment could have dramatic positive effects, it is
fundamentally an
evolutionary concept, not so much a revolutionary one.

More later. Thanks as always.

Lauren Weinstein <http://www.pfir.org/lauren> +1(818) 225-2800
lauren@pfir.org
Co-Founder, PFIR: People For Internet Responsibility - <http://www.pfir.org>
PRIVACY Forum - <http://www.vortex.com> Lauren's Blog: <http://lauren.vortex.com>

Re: USAF F-22 jets grounded by software glitch ([R 24 58](#))

<"Dr. Gregory Chapelle" <chapelle@ieee.org>>
Wed, 30 May 2007 09:04:39 -0700 (PDT)

This letter is to comment on a Risks to the Public article
published in May
2007 ACM SIGSOFT Software Engineering Notes. In particular my
comments will
address the article "USAF F-22 jets grounded by software glitch
([R 24 58](#))".

I believe your comment at the end of the article "However, the F-
22 Raptor
was presumably unwrapped without the benefit of raptor
simulation, testing,
and other preflight analyses. Perhaps the quality control is
going downhill"
was out of line. I personally worked on the Raptor Integrated
CNI
(Communications Navigation and Identification) system and can
attest that
extensive 4+ years of testing and analysis went into that system.

I think the fundamental "take away" from this is not "what a bunch of stupid idiots", but rather what was the basic development/testing process problem that allowed this issue to slip through. I think I can shed some light on this.

Basically with a complex system like this, the government (the Air Force in this particular instance) has detailed specific performance requirements that the system must meet. A great deal of design and testing go into verifying that the system meets these functional requirements. Even failure modes are addressed when resource sharing and detailed studies/testing are performed to keep classified operational computer data from being accidentally released into the unclassified processors. Extensive operational scenarios were developed, and detailed Rate Monotonic Analysis were performed for each of these.

The hardest part in trying to meet these large number of requirements is to step back and say "what have I forgotten to test for". It's easy to test and identify the written requirements in front of you, but much more difficult to identify less obvious failure modes.

The real kicker for most people when learning of this reported error is how obvious it is in hindsight. Why didn't we test for this obvious operational mode of crossing the international date line? This is probably the second "take away" from this error. For Navigation, an accurate time reference is the key that unlocks everything. We tested for timing errors in GPS,

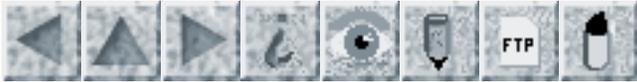
requisition of time if it was lost, and numerous other "time" type of errors. We were confident that we had addressed any time reference errors, but we never specifically addressed the International Date Line. In the rush to verify functional requirements, we did not look carefully at our testing coverage, and because we danced around similar failure modes, we were confident that we had "covered all our bases". Again, I would say if we had stepped back and took a careful look at the "completeness" of our testing, we might have identified this hole.

So where does that put us today. I think today the pressures on software development to produce and test faster prevents a "stand down" moment. The fast pace does not allow reflective contemplation for an overall view of a project's objectives and to confirm adequate design and testing. As systems become more complex there comes a need for a group/person separate from the design group to cast an impassionate eye over things and independently verify that there are no "unresolved operational issues".

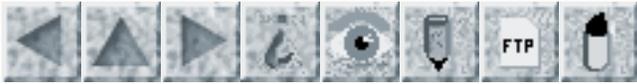
While I no longer work for the Integrated CNI group, I continue to work on government programs and even with 20+ years of experience strive to improve and do better. I always find your "Risks to the Public" engaging and unnerving at the same time. I share pertinent articles my design teams and will be discussing the F-22 one with them too!

Thank you for helping to make software systems better.

Dr. Gregory Chapelle <chapelle@ieee.org> 858.676.7361 (work)



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 71

Tuesday 26 June 2007

Contents

- [DHS = Department of Holey Security?](#)
[PGN](#)
- [United Airlines cites 'human error' for glitch](#)
[Mark J Bennison](#)
- [Cause of Gripen "spontaneous ejection"](#)
[Paul E. Black](#) [Crispin Cowan](#)
- [Transport system complexity presents insurmountable risk?](#)
[Mike Martin](#)
- [Improving reliability of critical software](#)
[Jeremy Epstein](#) [Paul E. Black](#)
- [More people die from sand hole collapses than sharks](#)
[Jeremy Epstein](#)
- [E-vote 'threat' to UK democracy](#)
[David Lesher](#)
- [Reality TV, video archives and on-line voting](#)
[Robin Fairbairns](#)
- [A movie torpedoed the concept of electronic voting?](#)
[Ferdinand J. Reinke](#)

- [Information leaked from web order page](#)
[Bruce Hamilton](#)
 - [Not much e-mail is protected from government search](#)
[Andrew Klossner](#)
 - [Re: Search Engine Dispute Notifications](#)
[Crispin Cowan](#)
 - [Advertising Risk](#)
[Rob Boudrie](#)
 - [Not Talking About vs. Not Doing](#)
[Gene Wirchenko](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ DHS = Department of Holey Security?

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

Wed, 20 Jun 2007 18:12:36 PDT

[See my recent testimony on Security and Privacy in the
Employment
Eligibility Verification System (EEVS), for a hearing of the
House Ways
and Means Committee Subcommittee on Social Security:
<http://www.csl.sri.com/neumann/house07.pdf> and
[http://www.acm.org/usacm/PDF/
EEVS_Testimony_Peter_Neumann_USACM.pdf](http://www.acm.org/usacm/PDF/EEVS_Testimony_Peter_Neumann_USACM.pdf)

DHS is responsible for EEVS. The prototype has a four-percent
error rate
overall, which is reportedly much higher among eligible would-
be employees
who are not U.S. citizens. PGN]

"Homeland Security Department computers and cyber systems have
been infected
with viruses and malicious scripts that could compromise
passwords and
information on U.S. citizens, intelligence operations and the
nation's

critical infrastructure. ... A draft report from the Homeland Security Department's inspector general found that two computer systems at the department's headquarters were infected with scripts that could compromise passwords and allow unauthorized access by outsiders." [Source: Chris Strohm, CongressDaily, 19 June 2007, PGN-excerpted.]
<http://govexec.com/dailyfed/0607/061907cdpm2.htm>

[The article by Chris Strohm was written in anticipation of another hearing by the same subcommittee on the same subject. Annie Anton's written testimony for that hearing is also online:
http://www.acm.org/usacm/PDF/SSN_Anton_USACM_testimony.pdf
PGN]

United Airlines cites 'human error' for glitch

<"Bennison, Mark J" <mark.m.bennison@mbda.co.uk>>
Fri, 22 Jun 2007 07:49:21 +0100

'Chief Operating Officer Pete McDonald said the error occurred during routine system testing. "Yesterday, an employee made a mistake and caused the failure of both Unimatic and our backup system," he said in the recorded call to employees. He did not elaborate on the error.'

For such a critical system one wonders why both the main and backup system failed as a result of the mistake - indicating a lack of robustness in the system design to me - but moreover why "routine system testing" was being

performed on a live system during peak times? In the UK I believe that system testing (and upgrades etc) of airline computer systems occurs overnight (OK, the concept of 'overnight' for a worldwide system is moot, but it is performed at times of least activity).

[See also an earlier report from 20 Jun 2007,
Computer outage grounds United for 2 hours

<http://www.cnn.com/2007/TRAVEL/06/20/united.flights.ap/index.html>

PGN]

⚡ Cause of Gripen "spontaneous ejection" (Re: Lima, [RISKS-24.70](#))

<"Paul E. Black" <paul.black@nist.gov>>

Thu, 21 Jun 2007 13:44:25 -0400

A comment on the article by "maddogone" says, "The tests show it was the G-suit which activated the ejection. ... when it filled with air it pressed against the release handle"

For an explanation of an anti-G suit, see

<http://www.daviddarling.info/encyclopedia/A/antigsuit.html>

⚡ Cause of Gripen "spontaneous ejection" (Re: Lima, [RISKS-24.70](#))

<Crispin Cowan <crispin@novell.com>>

Wed, 20 Jun 2007 10:41:20 -0700

Is this really a case of complex systems interaction producing unpredictable results? Or is it that high G-forces tripped the switch to induce ejection? The latter is just defective design of a single component with respect to the environment it was intended for.

Crispin Cowan, Ph.D., Director of Software Engineering <http://novell.com>

AppArmor Chat: <irc.oftc.net/#apparmor> <http://crispincowan.com/~crispin/>

✶ Transport system complexity presents insurmountable risk?

<"mike martin" <mke.martn@gmail.com>>

Thu, 21 Jun 2007 18:05:09 +1000

How difficult is it to collect a bus fare or commuter rail fare?

The state of New South Wales was to have an integrated, smartcard-based ticketing system covering all modes of public transport other than taxis, in time for the Sydney 2000 Olympic Games.

The system is still not working. A recent pilot trial in buses was called off when the 420 bus drivers involved voted to boycott it. The ticket machines kept crashing and bus drivers had to stop each time to fix them, <http://www.smh.com.au/news/national/driver-boycott-delays-tcard-once-again/2007/06/14/1181414469692.html>

All well and good; it sounds like any number of other projects where governments have been let down by technology. There is an oddity

here
though. The firm selected to provide the ticketing system, ERG Group, has
been a partner in over a dozen successful projects around the world,
including the Hong Kong Octopus system, claimed to be the largest of its
type. It has supplied similar ticketing systems in San Francisco and
Washington, DC. What's unique about NSW that has caused such protracted
delays?

Yesterday a report in The Australian Financial Review (unavailable online) gave a hint as to what the real problem is:

"Transport experts have repeatedly warned that NSW's more than 70 individual public transport fare products is unnecessarily large and will require dramatic simplification in order for an integrated ticketing system to be successful across all modes of transport.

"The NSW government conceded yesterday that it would need to substantially simplify fare structures to make the Tcard project a reality. The most likely option was a system of distance-based zones similar to that of most other metropolitan transport authorities."

It is 11 years since the Public Transport Authority of NSW was set up to pursue integrated ticketing as a means of increasing the attractiveness of public transport. It appears that the government may have finally realised what "integrated" really means.

Mike Martin, Sydney <mke.martn@gmail.com>

✦ Improving reliability of critical software (Re: Auslander, [R-24.70](#))

<"Jeremy Epstein" <jepstein@webmethods.com>>

Thu, 21 Jun 2007 12:28:42 -0400

It's a very appealing idea, but one that doesn't work. N-version programming has been studied, and the essential problem is that the teams tend to make the same mistakes, and also that determining a "mismatch" is harder than it sounds. See J. C. Knight and N. G. Leveson. "An experimental evaluation of the assumption of independence in multiversion programming". In IEEE Transactions on Software Engineering, SE-12 (1):96-109, January 1986.

There's a good summary of the issues at http://en.wikipedia.org/wiki/N-Version_Programming.

Take as an example the problem of building a browser, which I'd argue is one of the biggest real-world N-version programming examples ever tried: there are some reasonably detailed specifications as to protocols (e.g., HTTP), layout (e.g., HTML), etc. - but there are many web sites that work (or look "right") with one but not another browser - even setting aside features specific to one browser (such as ActiveX). A decision function would have a very difficult time deciding whether the browsers give consistent results for the specifications.

>The space shuttle software has used this technique for quite a while.

The Space Shuttle does **not** use N-version programming - it uses identical instances of the same software, and uses redundancy to account for hardware failures. Again, a good explanation of the methodology used is at http://en.wikipedia.org/wiki/Space_shuttle.

The RISK? Assuming that having multiple independent version is going to solve mission critical reliability problems!

✦ Improving reliability of critical software (Re: Auslander, [R-24.70](#))

<"Paul E. Black" <p.black@acm.org>>

Thu, 21 Jun 2007 14:31:00 -0400

N-version programming to improve reliability of critical software?

N-version programming may lead to much higher quality IF errors are independent. Hatton 1997 cites studies that support sufficient independence. Brilliant, Knight, and Leveson 1990 reported that in an experiment programmers made "equivalent logical errors" and different logical errors caused "statistically correlated failures". So it is no panacea.

✦ More people die from sand hole collapses than sharks

<"Jeremy Epstein" <jepstein@webmethods.com>>

Thu, 21 Jun 2007 08:26:19 -0400

Interesting article comparing the number of people killed in the US each year from the collapse of sand holes (i.e., holes dug in the beach) vs. shark attacks. A good explanation that people are "People naturally worry about splashier threats, such as shark attacks. However, the Marons' research found there were 16 sand hole or tunnel deaths in the United States from 1990 to 2006 compared with 12 fatal shark attacks for the same period".

This echoes a point frequently made in RISKS, so it should be no surprise to any readers here.

Will legislators call for laws to improve safety and protect against terrorists by banning sand?

Full article:

<http://www.cnn.com/2007/HEALTH/06/20/sand.deaths.ap/index.html>

E-vote 'threat' to UK democracy

<David Leshar <wb8foz@panix.com>>

Mon, 25 Jun 2007 09:37:54 -0400

E-vote 'threat' to UK democracy

Ballot boxes, BBC

Observers saw big problems with e-counting systems

British democracy could be undermined by moves to use electronic voting

in elections, warns a report.

<http://news.bbc.co.uk/1/hi/technology/6229640.stm>

The risks involved in swapping paper ballots for electronic versions far outweigh any benefits they may have, says the Open Rights Group report.

Technical chaos hits local counts ballot box Technical difficulties blighted the counts in the west of Scotland Voters in the west of Scotland have been hit by chaos during the Scottish parliamentary elections.
http://news.bbc.co.uk/2/hi/uk_news/scotland/glasgow_and_west/6623239.stm

Counts in Argyll and Bute, Eastwood, and Strathkelvin and Bearsden were suspended until later on Friday due to technical problems.

The problem at the Strathkelvin and Bearsden count occurred when the computer system could not validate the votes that had been counted so far.

http://news.bbc.co.uk/2/hi/programmes/click_online/3945675.stm

America's presidential election could be one of the closest in history, and in the past four years there has been a great deal of pressure to come up with a foolproof, electronic voting system. Ian Hardy reports on whether or not that has been achieved.

Debate about e-voting technology may be only just beginning According to officials in Fairfax County, the latest e-voting technology is simple, straightforward and sure-fire.

The county's electoral official, Blanche Kapustin, says: "When they look at the screen they'll see that the name of the person they've selected has

turned red. There's also a gigantic tick mark next to that person's name.

"They return to the summary screen, press the "next" button and once they press the "vote" button that's the end."

The data, which is collected on a memory device, is taken to a central location to be processed.

But opponents of e-voting say the current system is fundamentally flawed because there is no way that a voter's intent can ever be proved by anyone, once they have walked away from the screen.

⚡ Reality TV, video archives and on-line voting

<Robin Fairbairns <Robin.Fairbairns@cl.cam.ac.uk>>

Thu, 21 Jun 2007 17:44:26 +0100

One of the (apparently) less offensive sorts of reality TV in the UK is the show where someone is chosen to perform a part in an upcoming stage production.

The BBC was doing one to choose a leading man for a new West-End production of "Joseph and his amazing technicolour dreamcoat", and they had the rather pleasing idea of finding a children's choir to perform alongside the chosen singer in the final. The choir was to be made up of children no older than 11; the world at large was to get the opportunity of voting on 1-minute video clips of schools, and one of those voted into the top 20

would then be
chosen by Andrew Lloyd Webber himself (the composer of "Joseph").

Cue frenzy among the primary-school music teachers of the UK.
Existing
school choirs started learning the music for their clip; a fair
few schools
decided to form a choir of their own; arrangements had to be
made for
recording the clip, and so on, and so on. This was all to the
good:
everyone (who cares) is worried about music in British schools,
and here was
real motivation.

But then it started to go wrong. Very soon after the first
schools had
uploaded their clips, it was clear that the server wasn't sized
for the
demands that were to be placed on it. The first time I looked
at the site,
there were several-minute delays each time I asked for another
performance
to consider; there were less than 200 clips on line, at the
time, and voting
hadn't yet started.

It was clear the BBC hadn't realised the reaction they were
going to get.
For every school that entered a choir, there were 20 children,
the
children's families, the school's teachers, and assorted hangers-
on like me
(my wife is a teacher). Nearly 850 schools had entered, by the
end.

The voting scheme was that each vote had to give a choir a score
in the
range 1-5; places were to be decided by the choir's "average"
score over all
votes they had received. Each voter could vote for as many
choirs as she
had time for. None of the organisers seems to have considered

the obvious
weakness of such a voting system.

Voter registration seems to have been on the basis of IP address
-- a blow
for schools (or homes) all of whose computers are NAT-addressed,
and for
homes where there's only one computer with several users.

Within a few days of the server operating by fits and starts,
they closed
the voting and said they were thinking again. When voting
restarted,
registration was by email address/password, entering those on-
line on the
Joseph site -- something I suspect will have been a disincentive
to some.
The site was, however, responsive at this stage.

But even though voting was underway again, it was clear that not
all was as
it should be. The "top 20", which appeared on your screen
whenever you
connected, hardly seemed to move though some of them were, in
all honesty,
less deserving than many of those further down the table.

The BBC blamed the voters. "Block voting", they said, was the
order of the
day; but it's impossible to know what was actually happening
since the BBC
weren't forthcoming about the details. (It has to be said that
the site
managers -- BBC contractors, not BBC people -- responded
promptly to
reasonable enquiries.)

Eventually, even the BBC seemed to agree that even the revised
voting system
was not fit for purpose. Having delayed beyond their original
deadline for
announcing the finalists, they admitted defeat on the on-line
voting, and

closed the voting site. They recruited a panel to view all the clips to choose the top few for Lloyd Webber to review.

The school that was finally chosen hadn't appeared near the top on-line, and I, for one, didn't see its clip. One hopes it was better than all the *extremely* good schools I viewed, but since the BBC withdrew all clips when they gave up on the voting, I shan't ever know. And I don't have a TV, so I never saw them performing at all.

Oh, and my wife's choir was far lower in the voting than it merited. (I have to admit that though it's good, it wasn't up there with the very best.) I gave it 5...

Risks: well, lots. Don't underestimate the popularity of your site. Don't invent crooked voting systems; don't try to rehash your voting system on the fly. In short: accept that this sort of thing isn't "easy".

Of course, we don't know what advice the BBC had, so we'll never know if the cause was the BBC managers rejecting advice on cost grounds, or their software contractors getting the design wrong. I can guess a scenario, but I wouldn't care to publish it.

Robin Fairbairns -- University of Cambridge Computer Laboratory

⚡ A movie torpedoed the concept of electronic voting?

<"r @ reinke" <reinke@reinke.cc>>
Sun, 24 Jun 2007 00:39:08 -0400

Man of the Year, with Robin Williams as President Elect Tom Dobbs

Tom Dobbs, comedic host of a political talk show - a la Bill Maher and Jon

Stewart - runs for President of the US as an independent candidate who,

after an issues-oriented campaign and an explosive performance in the

final debate, gets just enough votes to win. Trouble is he owes his

victory to a computer glitch in the national touch-screen voting system

marketed by Delacroy, a private company with a rising stock price. To

protect their fortune, Delacroy executives want to keep the glitch a

secret, but one programmer, Eleanor Green, wants Dobbs to know the

truth. Can she get to him? Written by jhailey.

<http://www.imdb.com/title/tt0483726/>

Correct me if I am wrong, but did this movie just put a stake thru the heart of the vampire known as "electronic voting"?

Systems provided by Delacroy ... err I mean Diebold ... could manipulate the results of an election. Based on the movie, I've just emailed Ron Paul to change his name to Ron Paaul. (SPOILER: In the movie, the buggy computer program elects the candidate with the "best" double letter.) So if anyone wants to debate about paperless electronic Internet voting and tell you how good it will be yada yada yada, just rent them this movie. That should finish up the discussion!

They say many a true word is said in jest.

Some times concepts can get thru via humor. My non-techie spouse said after watching this that it would now never be approved here. Hope she's right.

This film IMHO says it all about that topic. And, says it in way that comes across to the average person.

p.s.: The movie did have one other great line. Tom Dobbs says "Politicians are a lot like diapers. They should be changed frequently, and for the same reasons." If you gather I'm no fan of politicians, you're correct. They are like diapers!

Ferdinand J. Reinke, Kendall Park, NJ 08824 <http://www.reinke.cc/>
<http://www.reinkefaceslife.com/> <http://www.linkedin.com/in/reinkefj>

[Well, the script writers for the film relied on a plot hook relating to a rather amusing accidental misprogramming rather than a Trojan horse. The latter might have been more effective in making the case. Incidentally, we don't generally reveal plot hooks in RISKS. However, this film has been around long enough (for example, it's been on several flights with me well after I had seen the first run). PGN]

Information leaked from web order page

<<bruce_hamilton@agilent.com>>
Thu, 21 Jun 2007 11:09:22 -0600

I just placed an order with MYSTICMAID (www.mysticmaid.com). One checkout step was to fill in the usual - name, address, email, phone, etc. The page offered to me was already filled in with someone else's information! A quick check showed that the phone number matched the name; I suspect that the address, email and other items matched also.

The shopping cart software let me use that information to proceed with the purchase, but the credit card number was not pre-filled in :-)

At least the person I called at the company expressed concern and said they would look into it.

bruce_hamilton@agilent.com Tel: +1 408 553 2818 Fax: +1 408 553 3487
Agilent Technologies MS 4U-SM P.O. Box 58059, Santa Clara, CA 95051-7201

⚡ Not much e-mail is protected from government search

<Andrew Klossner <andrew@cesa.opbu.xerox.com>>
Wed, 20 Jun 2007 13:24:36 -0700

The EFF press release starts out "San Francisco - The government must have a search warrant," but in fact the ruling does not apply in San Francisco. It applies only in Kentucky, Michigan, Ohio, and Tennessee, the states in the jurisdiction of the Sixth District Court of Appeals.

If the ruling is appealed to the Supreme Court, their judgment will apply to the entire country.

✶ Re: Search Engine Dispute Notifications (Weinstein, [RISKS-24.70](#))

<Crispin Cowan <crispin@novell.com>>

Wed, 20 Jun 2007 15:36:28 -0700

I see a simple solution to this problem: individuals who feel defamed by slanderous web sites just need to copyright or otherwise classify that information about themselves as intellectual property, and then issue a DMCA take-down order. :-)

Crispin Cowan, Ph.D., Director of Software Engineering <http://novell.com>

AppArmor Chat: <irc.oftc.net/#apparmor> <http://crispincowan.com/~crispin/>

✶ Advertising Risk

<"Rob Boudrie" <rob@boudrie.com>>

Fri, 22 Jun 2007 10:53:27 -0400

The recent disaster at Six Flags/KY where a kid had his feet severed by a ride shows the risks of automated ad selection systems. I viewed the video of the story at on-line on a KY tv station, and there was the typical automatically selected commercial one had to watch to get to the story. The commercial was an ad for the same Six Flags amusement park

covered in the
story.

⚡ Not Talking About vs. Not Doing

<Gene Wirchenko <genew@ocis.net>>

Wed, 20 Jun 2007 17:36:11 -0700

<http://thomascrampton.com/2007/06/15/perils-of-privacy-on-facebook/>

covers an interesting risk regarding a status change. The key part:

'My fiancée and I decided that showing our engagement in Facebook gave out a little too much personal information.

But I did not realize that unchecking the box marked "Thomas Crampton is engaged to Thuy-Tien Tran" would send a message to everyone connected to us in Facebook that "Thomas Crampton and Thuy-Tien Tran are no longer engaged".'

Complications ensued.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 72

Wednesday 11 July 2007

Contents

- [Remote physical security for air traffic control center](#)
[Rob Slade](#)
- [Beware of the fine print](#)
[Peter Mellor](#)
- [The risk with the Mac OS X 10.4.10 version number](#)
[T Yip](#)
- [The Athens Affair: Greek Cellphone Caper](#)
[Roy Stehle](#)
- [Lightning bolt blamed for NYC power outage](#)
[PGN](#)
- [Voltr Risks, Glitch - Fire Alarm - International Space Station](#)
[Robert J Perillo](#)
- [Wikipedia, It's Time to Grow Up! The Benoit Murder/Suicide Case](#)
[Lauren Weinstein](#)
- [Wikipedia and Responsibility](#)
[Lauren Weinstein](#)
- [Re: Transport system complexity presents insurmountable risk?](#)
[Mark Brader](#)

- [Re: Gripen: Risks of safety measures in military jet aircraft](#)
[Matt Jaffe](#) [Peter Mellor](#)
 - [N-version programming -- the errors are in ourselves](#)
[Fred Cohen](#)
 - [Secure Programming with Static Analysis](#)
[Brian Chess](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Remote physical security for air traffic control center

<Rob Slade <rMslade@shaw.ca>>
Mon, 09 Jul 2007 14:31:18 -0800

Because watching a monitor from 4,600 kilometres away is more secure ...

"The air traffic control center in Surrey, B.C. will have its security guards replaced with automated entry systems and officials watching monitors in Ottawa." CBC News, 9 Jul 2007

<http://www.cbc.ca/canada/british-columbia/story/2007/07/09/bc-airtrafficsecurity.html>

rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>

⚡ Beware of the fine print

<MellorPeter@aol.com>
Wed, 11 Jul 2007 08:27:52 EDT

On BBC Radio 4 "You and Yours" last week with a follow-up at lunchtime today (11th July 2007):

Some naughty web users have got more than they bargained for when casually browsing for adult material. At least two porn sites (mysexworld and sexpassport) feature a novel way of enforcing payment. A page on the site (p7 of 13 in one case) contains a warning well buried in the small print that, by visiting that page, the reader agrees to a 3 day free trial. If they do not cancel the arrangement, then a 3 month contract at 39.99 pounds payable in advance comes into force. It is stated that, if payment is not received, then the "subscriber" agrees to inconvenience up to and including the complete disruption of their use of their computer.

Having inadvertently walked into this "agreement", the hapless victims then found that they had downloaded software which flashed pop-up windows onto their screens, demanding payment. The pop-ups cannot be disabled, moved, closed or sent to background, and persist for increasingly long periods of up to 10 minutes. Since they appear every few seconds, they render the computer unusable.

This charming "business model" is the brainchild of a certain MBS, who lease the software to the porn site operators. The CEO of MBS quite brazenly stated that this is fair practice since the victims had knowingly agreed in advance to the disruption in the event of them not paying for their

subscriptions. He denied that he was anything to do with the porn "industry" and that his software was available for hire by any outfit wanting to sell any type of web services.

The UK Trading Standards Authority has received 200 complaints so far and are apparently "in discussion" with MBS to modify their practices. The equivalent authority in the US has adopted a less limp-wristed attitude and has enforced on a similar firm in the US a maximum duration of 40 seconds for the pop-ups, and are considering slapping an injunction on them to ban the practice.

To listen again to the programmes, go to <http://www.bbc.co.uk/radio4/youandyours/> and follow the links.

Peter Mellor; Mobile: 07914 045072; email: MellorPeter@aol.com

✶ The risk with the Mac OS X 10.4.10 version number

<T Yip <nyip10@yahoo.com>>
Thu, 28 Jun 2007 12:59:59 -0700 (PDT)

<http://www.macfixit.com/article.php?story=20070628105254900>

Mac OS X 10.4.10 is the first iterative release of Mac OS X to have 5 digits in its version string (1, 0, 4, 1, 0). It is also the first iterative release of Mac OS X to use the ".10" extension. This is causing some

significant issues.

The initial three [sic] digits for "10.4.10" are the same as "10.4.1," an earlier release of Mac OS X 10.4 (Tiger). Since the "MAC_OS_X_VERSION_ACTUAL" string (used by Cocoa applications to determine the current OS version) can carry a maximum of four digits, Mac OS X 10.4.10 and 10.4.1 are both labeled "1041."

This means that some applications recognize Mac OS X 10.4.10's version string as Mac OS X 10.4.1 and refuse to properly run, erroneously thinking that the system version is too old. For instance, the application UNO requires Mac OS X 10.4.4. When running under Mac OS X 10.4.10, it recognizes the Mac OS X version number as 10.4.1 and refuses to operate.

Essentially, the built-in Cocoa method for forbidding an app to run on too low a system breaks against Mac OS X 10.4.10.

We're still searching for a viable method for tricking applications into thinking that the system version is 10.4.9, which would largely obviate this problem.

RISKS: This sounds almost like a repeat of the Y2K scenarios, with all its attendant risks.

The Athens Affair: Greek Cellphone Caper (IEEE Spectrum)

<Roy Stehle <roy.stehle@sri.com>>

Mon, 02 Jul 2007 14:33:49 -0700

This is an interesting article. One would wonder what might be gained if the high-level parties were trained to know the insecurity of the cellular network. However, there's real life, and people will do what's convenient.

The Athens Affair

Vassilis Prevelakis and Diomidis Spinellis, IEEE Spectrum, July 2007

<http://www.spectrum.ieee.org/jul07/5280>

A case involving hackers deploying sophisticated eavesdropping technology within Greece's largest cellphone network provides a rare glimpse into one of the most elusive of cybercrimes. Major network penetrations of any kind are exceedingly uncommon. They are hard to pull off and equally hard to investigate. This one proved to be legendary.

[See the blogs of Matt Blaze and Steve Bellovin for excellent commentary:

<http://www.cs.columbia.edu/~smb/blog/2007-07/2007-07-06.html>

and

http://www.crypto.com/blog/hellenic_eavesdropping/

PGN]

⚡ Lightning bolt blamed for NYC power outage

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

Fri, 29 Jun 2007 13:10:15 PDT

On 27 Jun 2007, lightning hit a component of New York City's power distribution network, resulting in a 49-minute power outage that

affected

385,000 people in Manhattan's Upper East Side and the Bronx -- all supplied

by two power stations in the southwest Bronx that were knocked out. The

initial guess is that the system misdiagnosed the power surge resulting from

the lightning strike, and overreacted -- protectively shut down those

customers.

Following last summer's 9-day outage in Queens ([RISKS-24.36](#)),

Con Ed has

spent \$90 million to upgrade the aging equipment. [Source:

Patrick

McGeehan, *The New York Times*, National Edition, A25, 29 Jun 2007, PGN-ed]

⚡ Voltr Risks, Glitch - Fire Alarm - International Space Station

<Robert J Perillo <gibraltar_perillo@yahoo.com>>

Thu, 5 Jul 2007 16:22:23 -0700 (PDT)

The so-called "software glitch" that caused the false Fire Alarm to go off

in the Russian portion of the International Space Station (ISS) during the

major computer and solar panel position repairs in early June, was probably

not a glitch but a fail safe programmed response to the power failures being

experienced. (Since no one seems to know the detailed design of the Russian

systems, there is a slight possibility that it was a pre-programmed

response, or caused by, the computers going down, but the timing of the

alarm does not support this.)

We (U.S. Industry) used to program facilities monitoring systems, security, fire, heating-cooling, like that in the '70s and '80s, that is, the alarm would go off if power failed, dipped, or was irregular in a section, just to be on the safe side, i.e. if the fire alarm is not working, turn on the fire alarm. Now we are more sophisticated, and with battery or backup power on the main monitoring section, and more sophisticated software to detect a specific problem, to work around, and fault isolation software, this procedure is not in place any more. We have accurate Fire Alarms and an alarm to say the fire alarm is not functional, and power or voltage reduction (Voltr) alarms, and have stopped using this indiscriminate "shotgun" approach of turning on the fire alarm to be on the safe side.

In cryptographic devices, because of the problems with "gate arrays" when voltage is irregular, and the fact that a clear text can never be permitted to go out on the cipher text output, if we detect a power loss, voltage dip or irregularity on the device or components around the device, a Voltr Crypto-Alarm is issued, and the cipher text output is immediately disconnected, and not reconnected until the alarm is checked (Cleared). When things stop working, like data links, or Radios, everyone suspects the encryption device, and does an alarm check to clear the crypto, sometimes that works and sometimes it doesn't because the problem is not with the crypto.

Built-in-test (BIT), fault detection, calibration, remote maintenance, and/or fault isolation, is not the stepchild, leave it to the Intern, embedded systems software anymore. In the U.S., it is mature, complicated, specialized software written by experts.

About the use of '70s and '80s technology in the Russian portion of the ISS, while this might be a good thing for mechanical systems, it is worrisome in terms of computers and software?

Robert J. Perillo, Principal Software Engineer
dockmaster_perillo@yahoo.com

🔥 Wikipedia, It's Time to Grow Up! The Benoit Murder/Suicide Case

<Lauren Weinstein <lauren@vortex.com>>

Fri, 29 Jun 2007 08:56:46 -0700 (PDT)

June 29, 2007

<http://lauren.vortex.com/archive/000256.html>

Greetings. After causing law enforcement and the news media to spin their wheels uselessly, a Wikipedia user has [a href="http://abcnews.go.com/Sports/story?id=3327310"](http://abcnews.go.com/Sports/story?id=3327310)apparently confessed to planting a rumor as fact on the Wikipedia page for wrestler Chris Benoit, claiming his wife was dead hours before the bodies of Benoit and his family were found.

The ease with which this was done by a still anonymous party, triggering investigations and consternation at a time that was already

intensely
emotional for everyone involved with the Benoit case,
demonstrates once
again a fundamental flaw in Wikipedia's usually anonymous, non-
moderated
editing framework for most Wikipedia pages.

The fact that such editing can usually be undone (and redone
later for that
matter) doesn't change the fact that Wikipedia can never be an
authoritative
source while it is subject to this kind of anonymous abuse --
whether by
jokesters out to get their kicks or well-meaning contributors
simply
unwilling to check their facts. Such events can easily turn
Wikipedia pages
into rumor and defacement billboards rather than encyclopedia-
quality
content. The damage is already done.

If Wikipedia expects to really be taken seriously in the long
run, it needs
to rethink its standards for item creation, modification, and
attributions.

Wikipedia, it's time to grow up.

Wikipedia and Responsibility

<Lauren Weinstein <lauren@vortex.com>>
Sat, 30 Jun 2007 12:13:02 -0700

Wikipedia and Responsibility
<http://lauren.vortex.com/archive/000257.html>

Greetings. In the wake of my recent posting regarding Wikipedia
and the

Benoit murder/suicide case (<http://lauren.vortex.com/archive/000256.html>),

I've received a number of responses that boil down to: "Why are you blaming Wikipedia for anything relating to this situation? Wikipedia isn't supposed to be authoritative."

I definitely agree that in a perfect world everyone would understand that Wikipedia is not authoritative -- and cannot be under its current structure.

But in the real world, Google searches on a vast array of topics will return Wikipedia articles as the top or near top results (and/or in other contexts), and a vast number of sites use Wikipedia entries as convenient explanatory text or links -- despite most Wikipedia entries' lack of attribution, lack of documented fact checking, and being subject to mutation and alteration at any time. But Wikipedia entries are free, they're easy to link to, and hell, if any particular Wikipedia page is wrong at any particular moment, people can always say "it's not my problem."

Unfortunately, it is not necessarily obvious to many Web users following such links -- or reading related excerpted texts -- that Wikipedia articles "aren't supposed to be authoritative." Many people who find their way to Wikipedia items or texts don't know what Wikipedia really is about, and many persons understandably assume it's like any other "real" encyclopedia (that is, authors attributed somewhere, facts get a modicum of checking at least most of the time, entries aren't subject to random editing on a whim, etc.)

The Wikipedia folks created the system under which they operate. They need to take some responsibility when that structure causes damage. This isn't the first example of Wikipedia abuse screwing around with people's lives.

I am frankly very tired of hearing some people use the Internet as an excuse for anonymous attacks and abuses, with it seems relatively few persons having enough guts to take responsibility for the impacts that then result.

We want to let people post anonymously, at least the pseudo-anonymity (subject to tracing in many cases) offered by the Internet? Fine.

Anonymous speech definitely has its role. But the buck has to stop somewhere, and these systems should not be an excuse for a hit and run mentality.

In most such cases a significant amount of the responsibility when damage occurs must rest on the publisher of the unattributed information, if they have voluntarily chosen to operate in that manner. I'm not talking about common carriers and ISPs. I'm referring to sites that set themselves up in a way that serves to isolate posters/editors of material in public forums from attribution.

Again, if you want to operate this way, that's a perfectly valid choice.

But realize that you're transferring part of the responsibility onto yourself. I do not believe that as a society we can accept the premise that

anonymous systems erase all aspects of responsibility from all involved parties.

In the current Benoit situation, I likely wouldn't throw the book at that hoax poster. It's easy to be suckered in by the "devil-may-care" attitude that Wikipedia tends to foster. The hoaxer didn't realize that, in this case, they were falling into a serious and painful trap.

Lauren Weinstein +1 (818) 225-2800 <http://www.pfir.org/lauren>
Lauren's Blog: <http://lauren.vortex.com> lauren@vortex.com or
lauren@pfir.org

⚡ Re: Transport system complexity presents insurmountable risk?

<msb@vex.net (Mark Brader)>

Tue, 26 Jun 2007 12:40:54 -0400 (EDT)

(Martin, [RISKS-24.71](#))

In contrast to Sydney with its ticketing system that tries to do everything and fails, we have this story from England about ticketing machines that try NOT to do everything, and succeed... in cheating the passengers.

<http://www.timesonline.co.uk/tol/news/uk/article1975243.ece>

Three key paragraphs:

The companies have chosen secretly not to programme their ticket machines

to sell the GroupSave fare, which is meant to be available to any group of

three or four people traveling after the morning peak. Under GroupSave,

when two adults buy tickets another two can travel free.

Staff at ticket

offices are obliged to sell the cheapest fare, including GroupSave, even

if passengers do not specifically request it. But the law does not extend to machines.

Passengers travelling alone are also unable to obtain the cheapest fares

from machines for some morning trains on which those fares are valid. The

fares can be obtained only from ticket offices. Only 44 of SWT's 177

stations have offices open for at least 12 hours a day. Another 105 have part-time ticket offices and 28 have no offices.

After being presented with the evidence gathered by The Times, SWT said

that it would consider reprogramming its machines to offer the GroupSave

discount. A spokeswoman added: "We are looking at adding more options,

but then we get advised that the machines are really complicated and people can't use them."

(At this point something might be said about overly complex fare structures,

but note that according to the description in this article, the group fare is not an "option" in any case.)

Mark Brader, Toronto, msb@vex.net

✉ Re: Gripen: Risks of safety measures in military jet aircraft

<Matt Jaffe <jaffem@cableone.net>>

Sun, 01 Jul 2007 20:12:00 -0700

In [RISKS-24.71](#) Paul E. Black quotes "maddogone" as saying,

"The tests show it was the G-suit which activated the ejection. ... when it filled with air it pressed against the release handle"

I was unable to find the original source of the maddogone quote (perhaps Mr. Black can provide a reference) but I am doubtful of the explanation in the maddogone quote. I am unfamiliar with the Gripen but back in my day, more decades ago than I care to think about, US ejections seats were; activated by handles of one sort or another and none of the handles; in the aircraft I am familiar with could be activated by simple pressure (of an inflating G-suit). I could be wrong (it's rare, but it's been known to happen ;-)) but I doubt that the Gripen ejection system would have been designed with that obvious a hazard, given that ejection seat technology has been fairly mature for quite some time now. Be nice to know more, particularly if I am correct and the ejection was not caused by a simple mechanical stupidity but by a more complex systems problem which we, the readers of this forum, would want to know more about. So, as noted, perhaps Mr. Black can provide the source of the maddogone quote or other pointer to further information. (Or just tell me that I'm wrong and the Gripen ejection system *can* be activated by simple pressure, in which case shame on Gripen -- or, more specifically, their ejection seat manufacturer).

✉ **Re: Gripen: Risks of safety measures in military jet aircraft**

<MellorPeter@aol.com>

Mon, 9 Jul 2007 18:40:14 EDT

The item by Tony Lima <tony.lima@csueastbay.edu> in [RISKS-24.70](#) was interesting. The following is an excerpt from my paper "CAD: Computer-Aided Disaster", High Integrity Systems Journal, Vol. 1, No. 2, 1994, pp 101-156.

(It was based on press reports at the time. Statements in double quotes below are from people who were quoted in the press articles. I have omitted the references, but will send the whole paper to anyone who wants it.)

The SAAB JAS 39 Gripen is one of the new generation of aerodynamically unstable fighters. It has no ailerons on the main wings, but uses a pair of smaller wings mounted forward to control its attitude. The FCS actively controls these and other surfaces to maintain stability. The FCS employs three digital computers, presumably in some fault-tolerant architecture.

(Precisely what this architecture is, is not clear from the reports.)

"It has to respond to signals within 200 milliseconds in order to maintain stability. If the digital system is disconnected, an analogue backup system ensures that the plane flies level but it is not then possible to manoeuvre. Since the centre of gravity lies behind the centre

of lift,

there is a tendency to lift the nose when control is lost."

On 2nd February 1989, the first prototype was coming in to land after its sixth test flight. On its previous five flights it had shown a tendency

to lateral instability. This time, it showed longitudinal instability,

pitching down, then sharply up, then down again to the extent that the

pilot could not recover control. The aircraft hit the runway, shearing

off the left main gear, bounced, skidded off the runway, turned through

180 degrees, struck the ground with its right wingtip, flipped over, and

came to rest on its back. Amazingly, the test pilot, Lars Radestrom,

walked away from the wreck.

The investigating committee concluded that the crash was due to a software

fault. The chairman, Olaf Forsberg, stated:

"The accident was caused by the aircraft experiencing increasing pitch

oscillations (divergent dynamic instability) in the final stage of

landing, the oscillations becoming uncontrollable. This was because

movement of the stick in the pitch axis exceeded the values predicted when

designing the flight control system, whereby the stability margins were

exceeded at the critical frequency."

Note that the software fault in question seems to be a requirements fault,

since a separate investigation by the JAS consortium concluded:

"The control laws implemented in the flight control system's computer had

deficiencies with respect to pitch axis at low speed. In this case, the pilot's control commands were subjected to such a delay that he was out of phase with the aircraft's motion. ... JAS is now introducing the necessary modifications to the control laws."

Just how effective these changes were is shown by the events of 8th August 1993, when the second production aircraft (out of 140 ordered by the Swedish Air Force) was engaged in a display flight over the Water Festival in Stockholm. Entering a turn, the pilot found that "... the computer overcompensated by roughly 10 degrees. When I then straightened out the aircraft, I got an undemanded pitch oscillation and, when I tried to compensate for that one, the aircraft kind of sat down and became impossible to control." He added that it felt "... like being on top of a slippery sphere" or "... like butter on a hot potato".

At the point when the aircraft reached a nose-up angle of around 70 degrees to the horizontal, the pilot decided to get out and walk. He ejected safely, and the aircraft then leveled off and flew on for a while before crashing on an island. The only casualties were one tree, three spectators who suffered minor burns, and one who sprained an ankle running away!

The Crash Investigative Commission stated in their preliminary report:

"The JAS crash was caused by the control system's high amplification of joystick deflections in combination with the pilot's large and

rapid

joystick movements. This caused margins of stability to be exceeded."

They also concluded that the aircraft had no technical faults at the time

of the accident. The engine continued to function normally until the

plane hit the ground. From loss of control until ejection had taken 6.2 seconds.

The cause of the crash was therefore "partly the pilot and partly the

control computer" (i.e., the FCS). The phenomenon is referred to as

"Pilot Induced Oscillation" (PIO). The cycle time of the Gripen FCS is

200 milliseconds, similar to the human sensory/motor system reaction time.

According to the report: "The designers knew that during certain

circumstances the aircraft could be forced into an unstable state due to

the steering-gear actions of the pilot, which would cause the aircraft to

leave its envelope. However, they had estimated the risk of this

happening to be very low. As it turned out, after some 7-8G manoeuvre,

when the pilot tried to re-stabilize the plane, his actions happened to

coincide with that of the computer and so the aircraft over-staggered."

There are several interesting points about these crashes. In both cases,

it appears that the FCS was doing what was specified but not what was

required. This is often the case with such accidents. Also the tendency

is to blame (at least partly) the pilot, although a better design of human

interface would seem to be necessary. The investigators

concluded that

"When [measures have been taken to prevent any future similar occurrence],

the Commission expect there to be no reason for continued grounding of the

JAS 39 Gripen." (Following a \$3.2 billion development investment, this

should come as no surprise!)

On a final note, the pilot in the 1993 Stockholm crash was ... Lars

Radestrom! (His personal private comments on the subject of active FBW

would make interesting reading!)

Peter Mellor; Mobile: 07914 045072; email: MellorPeter@aol.com

Telephone and Fax: +44 (0)20 8459 7669

N-version programming -- the errors are in ourselves

<Fred Cohen <fred.cohen@all.net>>

Tue, 26 Jun 2007 10:35:21 -0700

The problem with N-version programming for redundancy is not that the idea

is flawed -- but rather that those implementing it are not sufficiently well

educated in the subject matter to do the job right. There is a related

sub-problem -- our educational system produces programmers that are too

uniform -- something like the problem in a lack of diversity in our

programming languages and hardware and operating systems.

In most of the examples cited to show that N-version programming fails, the

programs are all written in the same language by people with

similar
expertise and background using the same development platforms
and operating
systems. The common errors they make are not examined as part of
quality
control, and it is foolish to act as if N-version programming
will eliminate
common-mode failures that can be readily detected by automated
tools -- such
as failure to check bounds and off-by-one errors in array
references.

The assumption of independence is indeed one that is commonly
violated --
not by the programmers as much as by those who decide to use N-
version
programming but only go half-way. It is not "appealing" in the
sense that it
is expensive -- more than N-times as expensive -- to write an N-
version
program as a single-version one. It is only worth it in cases
where the risk
justify the costs.

As an example, try writing the 5-version program using the
following
environments:

- * Lisp on a LispMachine -- programmers from a trusted systems
development group
- * Shell script on an AT&T Unix box (3B2 or so) -- political
science
students from Chinese university
- * C on a 68000 microprocessor -- no OS -- doctors from an Indian
medical
center
- * Java on OS-X (68K processor) -- electrical engineers from the
power
industry
- * Pascal on a Windows Intel box -- historians from a museum in
Cairo

Put each through formal code review and proof processes to

generate
mathematical demonstrations that each is correct in the relevant
senses from
the specification -- which of course has to be developed
redundantly as
well.

You will probably tell me that this is ludicrous, and I will
probably agree
-- that if you really wanted a trusted program and the fate of
the World
depended on it, you would want more versions with even more
diversity. But
that's exactly the point of N-version programming. The more
assurance you
want, the more diversity you need.

Fred Cohen & Associates 572 Leona Drive Livermore, CA 94550
1-925-454-0171 <http://all.net/>

✶ Secure Programming with Static Analysis

<Brian Chess <brian@fortifysoftware.com>>
Wed, 04 Jul 2007 20:30:14 -0700

Jacob West and I are proud to announce that our book, Secure
Programming
with Static Analysis, is now available.

<http://www.amazon.com/dp/0321424778>

The book covers a lot of ground.

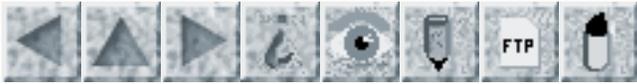
- * It explains why static source code analysis is a critical part
of a secure
development process.
- * It shows how static analysis tools work, what makes one tool
better than
another, and how to integrate static analysis into the SDLC.

* It details a tremendous number of vulnerability categories, using real-world examples from programs such as Sendmail, Tomcat, Adobe Acrobat, Mac OSX, and dozens of others.

[This is an extremely useful and timely book. 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

Search RISKS using [swish-e](#)

Volume 24: Issue 73

Tuesday 17 July 2007

Contents

- [CCTV biometric surveillance software fails German reliability test](#)
[Martin Virtel](#)
- [Military files left unprotected online](#)
[Randall via Dewayne Hendricks](#)
- [Face recognition flop](#)
[Christian Kutzt via Dave Farber](#)
- [Microsoft protects me against ... Microsoft](#)
[David de Leeuw](#)
- [Jogger with iPod Struck by Lightning](#)
[Gene Wirchenko](#)
- [Phone switch rootkit in Greek surveillance](#)
[Jeremy Kirk](#)
- [Space Shuttle uses 2-version programming](#)
[Andrew Morton PGN](#)
- [Re: N-version programming -- the errors are in ourselves](#)
[Peter Mellor](#)
- [Re: Gripen: Risks of safety measures in military jet ...](#)
[Henry Baker Peter Mellor](#)

- [Re: BSoD in standardized tests](#)
[Martyn Thomas](#)
 - [Re: Wikipedia and Responsibility](#)
[Joe Bednorz](#)
 - [Re: Risk with the Mac OS X 10.4.10 version number](#)
[Dirk Fieldhouse](#)
 - [Search Engine Dispute Notification](#)
[Jurek Kirakowski](#)
 - [Exploiting Online Games, Hoglund/McGraw](#)
[PGN](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ **CCTV biometric surveillance software fails German reliability test**

<"Martin Virtel" <virtel.martin@ftd.de>>

Thu, 12 Jul 2007 10:26:43 +0200

German federal police enrolled 200 commuters to test if they could use face recognition software to pick out suspects from a CCTV feed at a train station under real-world circumstances. The three systems tested (produced by Cognitec, Bosch and Cross Match) failed to recognize 8 out of 10 people they should have, even when they were fed images of people standing still on an escalator, one of the favourite settings for this kind of biometrics.

The key factor was the bad lighting conditions in the morning and afternoon, when most of the test suspects passed the cameras. (The test suspects were also fitted with RFID tags so they could be reliably identified by the test setting). Under the right conditions, the systems failed to recognize 4 out of 10 people, at a rate of 0.1 per cent of false alarms, which

the
researchers thought acceptable for practical police work.

The final report [German, link below] recommends against using the systems for identification purposes. They would only be useful under constant lighting conditions, and either openly seeking cooperation of the persons being checked by the biometrics software, or making them cooperate involuntarily, by using what the report calls "eye-catchers", like changing billboards or marquees. The report states that three-dimensional face recognition, currently being developed, could probably do better.

Although the report points out that the systems tested are basically not usable yet, there is still a major flaw in the design: The researchers thought 23 false alarms per day would be acceptable. If you have 23 false alarms a day, and only one or two real suspects (probably hiding their faces behind a newspaper) crossing the cameras per week, I think you would stop to trust the system very soon.

The final report (28 pages, german) is available here:
http://www.bka.de/kriminalwissenschaften/fotofahndung/pdf/fotofahndung_abschlussbericht.pdf

Martin Virtel, Redakteur Forschen & Entwickeln Fon: +49/40/319 90 469
Financial Times Deutschland GmbH & Co KG, Stubbenhuk 3, 20459 Hamburg;
Amtsgericht Hamburg HRA 92810 <http://www.ftd.de/forschung> virtel.martin@ftd.de

⚡ Military files left unprotected online (Randall via Dave Farber's IP)

<dewayne@warpspeed.com (Dewayne Hendricks)>

July 11, 2007 5:27:10 PM EDT

[Note: This item comes from reader Randall. DLH]

From: Randall <rvh40@insightbb.com>

Date: July 11, 2007 2:02:15 PM PDT

To: David Farber <dave@farber.net>, Dewayne Hendricks
<dewayne@warpspeed.com>

Subject: Oops.

Detailed schematics of a military detainee holding facility in southern Iraq. Geographical surveys and aerial photographs of two military airfields outside Baghdad. Plans for a new fuel farm at Bagram Air Base in Afghanistan.

The military calls it "need-to-know" information that would pose a direct threat to U.S. troops if it were to fall into the hands of terrorists. It's material so sensitive that officials refused to release the documents when asked. But it's already out there, posted carelessly to file servers by government agencies and contractors, accessible to anyone with an Internet connection.

In a survey of servers run by agencies or companies involved with the military and the wars in Iraq and Afghanistan, The Associated Press found dozens of documents that officials refused to release when asked directly, citing troop security. [Source: Mike Baker, Military files left unprotected online, AP item, 11 Jul 2007; PGN-truncated good long item, not

surprising]

http://news.yahoo.com/s/ap/military_online_insecurity;_ylt=Aixup_YEMhxbq7rTtPYTDaNhr7sF

🔥 Face recognition flop (via Dave Farber's IP)

<Christian Kuhtz <christian@kuhtz.com>>

July 11, 2007 2:32:40 PM EDT

Apparently the BKA (German equivalent of the FBI) tested face recognition, spent 200K euros to test the system in a rail terminal in the city of Mainz and basically declared it worthless in terms of being an investigative tool. Apparently (per the article) this is the first public trial under normal, every day conditions (rather than having the conditions manipulated for a good showing) and only matched 30%. Even when the lighting was modified to be ideal, it only reached 60%. The BKA considers the system only useful if the success rate is very near 100%.

The sample size was approximately 23,000 travelers per day over a period of roughly 3 months. The targets were 200 commuters who had volunteered for the trial and travel through this rail terminal at least once per day.

BKA recommended that this is not a suitable system for surveillance and facial recognition to try to match suspects in a manhunt etc.

The article is in German; try your favorite mechanized translator. If

there's enough demand, I happen to be bilingual and may be convinced into doing a translation in my spare time. ;-)

<http://www.spiegel.de/panorama/justiz/0,1518,493911,00.html>

Archives: <http://v2.listbox.com/member/archive/247/=now>

RSS Feed: <http://v2.listbox.com/member/archive/rss/247/>

Microsoft protects me against ... Microsoft

<David de Leeuw <ddl@medic.bgu.ac.il>>

Tue, 17 Jul 2007 08:07:19 +0200

After the latest monthly automatic updates for Windows XP, I got the following message on my screen:

Data Execution Prevention: Microsoft Windows

To help protect you computer, Windows has closed this program.

Name: Windows Explorer

Publisher: Microsoft Corporation

Data Execution Prevention helps protect against damage from viruses

and other security threats. What should I do?

Here is the screen picture:

<http://fohs.bgu.ac.il/bgu-med/pub/windowerror.jpg>

I will leave it to the Risks readers to find a creative explanation.

David de Leeuw, Medical Computing Unit, Ben Gurion University of the Negev
Beer Sheva, Israel

[Actually, a Beer sounds like a good idea,
after which you could Sit Shiva for your PC. PGN]

⚡ Jogger with iPod Struck by Lightning

<Gene Wirchenko <genew@ocis.net>>

Thu, 12 Jul 2007 21:09:00 -0700

A Canadian jogger happened to be carrying an iPod at the wrong place at the wrong time. Lightning struck his body during a thunderstorm, and the current ran along the path of the earphones and into his head, causing injuries to his jaw and ear eardrums. The patient's physicians say the combination of sweat and the metal earphones directed the current to his head.
<http://www.technewsworld.com/rsstory/58292.html>

⚡ Phone switch rootkit in Greek surveillance (Re: [RISKS-24.72](#))

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

Thu, 12 Jul 2007 11:10:18 PDT

Jeremy Kirk, Greek spying case uncovers first phone switch rootkit, 12 Jul 2007

http://news.yahoo.com/s/infoworld/20070712/tc_infoworld/90154

A highly sophisticated spying operation that tapped into the mobile phones of Greece's prime minister and other top government officials has highlighted weaknesses in telecommunications systems that still use

decades-old computer code, according to a report by two computer scientists.

The spying case, where the calls of around 100 people were secretly tapped, remains unsolved and is still being investigated. Also complicating the case is the questionable suicide in March 2005 of a top engineer at Vodafone Group in Greece in charge of network planning.

A look into how the hack was accomplished has revealed an operation of breathtaking depth and success, according to an analysis on IEEE Spectrum Online, the Web site of the Institute of Electrical and Electronics Engineers.

The case includes the "first known rootkit that has been installed in an [phone] exchange," said Diomidis Spinellis, an associate professor at the Athens University of Economics and Business, who authored the report with Vassilis Prevelakis, an assistant professor of computer science at Drexel University in Philadelphia.

A rootkit is a special program that buries itself deep into an OS for some malicious activity and is extremely difficult to detect. The rootkit enabled a transaction log to be disabled and allow call monitoring on four switches made by Telefonaktiebolaget LM Ericsson within Vodafone's equipment. The software enabled the hackers to monitor phone calls in the same way law enforcement would, minus the required court order. The software allowed for a second, parallel voice stream to be sent to another phone for monitoring.

The intruders covered their tracks by installing patches on the system to route around logging mechanisms that would alert administrators that calls were being monitored. "It took guile and some serious programming chops to manipulate the lawful call-intercept functions in Vodafone's mobile switching centers," the authors wrote.

The secret operation was finally discovered around January 2005 when the hackers tried to update their software and interfered with how text messages were forwarded, which generated an alert. Investigators found hackers had installed 6,500 lines of code, an extremely complex coding feat.

"The size of the code is not something that somebody could hack in a weekend," Spinellis said. "It takes a lot of expertise and time to do that."

The investigation, which included a Greek parliamentary inquiry, netted no suspects, due in part to key data that was lost or destroyed by Vodafone, the authors wrote. It's not known if the hack was an inside job.

Vodafone may have been able to discover the scheme sooner through statistical call analysis that could have linked the calls of those being monitored to calls to phones used to monitor the conversations, they wrote.

Carriers already do that sort of analysis, but more for marketing than security.

But the defense against rogue code, viruses and rootkits is complicated due to how telecom infrastructure has developed. "Complex interactions between

subsystems and baroque coding styles (some of them remnants of programs written 20 or 30 years ago) confound developers and auditors alike," the report said.

✈ Space Shuttle uses 2-version programming

<"andrew morton" <drewish@katherinehouse.com>>

Fri, 13 Jul 2007 12:22:05 -0700

> The Space Shuttle does **not** use N-version programming - it uses identical instances of the same software, and uses redundancy to account for hardware failures. Again, a good explanation of the methodology used is at http://en.wikipedia.org/wiki/Space_shuttle.

I wonder if Jeremy read the Wikipedia article he linked to... currently it reads:

"The Backup Flight System (BFS) is separately developed software running on the fifth computer, used only if the entire four-computer primary system fails. The BFS was created because although the four primary computers are hardware redundant, they all run the same software, so a generic software problem could crash all of them."

http://en.wikipedia.org/w/index.php?title=Space_Shuttle&oldid=141962184

✶ Space Shuttle uses 2-version programming

<Peter G Neumann <risko@csl.sri.com>>

Mon, 16 Jul 2007 13:38:40 PDT

As I understand it, the following is true: the FIFTH computer is not fully functional -- it is intended to have just enough programming to land the shuttle in the event that the four main computers all fail. Testing it safely under live conditions where the first four computers are inoperable is essentially undesirable, if not practically impossible. The fifth system has never been invoked. Worse yet, it has most likely not been maintained for compatibility with the other four. That is not what is generally thought of as N-version programming for N=2 in the realistic sense of the word, although it might be considered so for the stark subset of the functionality. It is more like a hot standby fail-safe mechanism.

✶ Re: N-version programming -- the errors are in ourselves

<MellorPeter@aol.com>

Sat, 14 Jul 2007 12:08:08 EDT

Regarding the thread in [RISKS-24.71](#) and 72, the results of Knight and Leveson's famous N-version experiment show that, if any three of the replicates from among those they had written were combined in a

two-out-of-three voting configuration, the resulting fault-tolerant system would have a probability of failure 19 times smaller than one of the replicates on its own.

This is not as much as fully independent failure would yield, but it is a significant improvement.

Peter Mellor +44 (0)20 8459 7669 Mobile: 07914 045072
MellorPeter@aol.com

✉ **Re: Gripen: Risks of safety measures in military jet ... ([R-24.72](#))**

<Henry Baker <hbaker1@pipeline.com>>

Thu, 12 Jul 2007 11:19:16 -0700

This delay-caused pilot-induced-oscillation reminds me of trying to drive some of the simulated vehicles in current video-game environments. The video (and other) effects are stunning, but the experience is marred by the delays between the controls and the perceived video. Unlike driving a real car at >100mph, for example, where the effects of control inputs are felt immediately, the control inputs in videogame-simulated vehicles have a noticeable delay. These delays can cause uncontrollable oscillations if not consciously damped by the gamer.

Analogously, a gamer who gets into a real car and attempts to go >100mph will find the opposite situation -- he is expecting a delay, but instead

gets instant (and potentially disastrous) results, compounded by the real inertia of his arms & legs interfering with any recovery effort.

✶ Re: Gripen: Risks of safety measures in military jet aircraft

<MellorPeter@aol.com>

Sat, 14 Jul 2007 11:52:49 EDT

In [RISKS-24.71](#) Paul E. Black quotes "maddogone" as saying,

"The tests show it was the G-suit which activated the ejection. ... when it filled with air it pressed against the release handle"

In [RISKS-24.72](#) Matt Jaffe <jaffem@cableone.net> quotes him and writes:

> I am unfamiliar with the Gripen but back in my day, more decades ago than
> I care to think about, US ejections seats were activated by handles of one
> sort or another and none of the handles in the aircraft I am familiar with
> could be activated by simple pressure (of an inflating G-suit).

In the early 1990's I spoke to a manufacturer of ejector-seats. Ejection was initiated by an upward pull on a handle positioned between the pilot's legs. The procedure was for the pilot to pull on the handle with the right hand, with the left hand gripping the right wrist. My contact explained that this was not because the handle was particularly stiff to operate (although it was not "hair-trigger") but in order to ensure that the pilot

took his left arm with him when he left.

Little chance of the inflation of a G-suit, or G-force alone, causing unintentional operation in that case. (I don't know if this applied to specifically to the Gripen.)

With aerodynamically unstable aircraft, the situation is different. If the FCS goes down, the aircraft might break up within half a second or so, depending on the airspeed and attitude, and I was given to understand that ejection would be automatic, i.e., initiated without manual input from the pilot.

Perhaps someone familiar with the Eurofighter could supply some authoritative information.

Peter Mellor +44 (0)20 8459 7669 Mobile: 07914 045072
MellorPeter@aol.com

Re: BSoD in standardized tests (Epstein, [RISKS-24.67](#))

<Martyn Thomas <martyn@thomas-associates.co.uk>>

Sun, 20 May 2007 09:00:42 +0100

Jeremy Epstein wrote " ...the RISKS of relying on systems that may not have been fully tested are pretty obvious."

This comes up far too often.

How would you know a system had been fully tested?

How long would it take?

Can you think of a better way to avoid system failures than test-

and-fix for a period of decades or more?

Testing is important for two main reasons:

to try to validate the assumptions you have made about the system's environment; to detect systems that are egregiously bad, so that you can scrap them and start again.

Computer scientists and programmers were saying all this 25 years ago. We won't improve much on the current failure rates of projects until we accept it, and act on it.

✈ **Re: Wikipedia and Responsibility (Weinstein, [RISKS-24.72](#))**

<Joe Bednorz <ign_strap@sbcglobal.net>>

Sat, 14 Jul 2007 17:44:05 GMT

* Immediate irresponsible editing, hugely magnified by Google, drives Wikipedia.

* Wikipedia survives through advanced blame-shifting. (Credit Seth Finkelstein for that insight.)

Changing either would destroy Wikipedia.

Why that won't happen:

* "One character who's laughing all the way to the bank, though, is Wales himself." ¹

* "Almost all of Wikipedia's 1,000-odd "administrators" receive

no pay for

their hard work other than the pleasure of power tripping -
seeing nothing

of the \$14m of VC money Wikipedia co-founder Jimmy Wales has
banked." ²

1. "Wikipedia defends Reality", from The Register.

<[http://www.theregister.co.uk/2007/02/02/
colbert_wikipedia_reality/](http://www.theregister.co.uk/2007/02/02/colbert_wikipedia_reality/)>

2. "Farewell, Wikipedia?", The Register

<[http://www.theregister.co.uk/2007/03/06/wikipedia_crisis/
page3.html](http://www.theregister.co.uk/2007/03/06/wikipedia_crisis/page3.html)>

✉ **Re: Risk with the Mac OS X 10.4.10 version number (Yip, [RISKS-24.72](#))**

<"Dirk Fieldhouse" <fieldhouse@gmx.net>>

Thu, 12 Jul 2007 13:15:32 +0100

I have several counter-risks here:

* writing applications that ignore the known (perhaps sometimes non-trivial)

best practice, which is to detect the capabilities required by the

application (and which, as I discover, has been supported by the Gestalt()

API since Classic OS 6.0.4)

[http://developer.apple.com/documentation/Darwin/Reference/
Manpages/man3/Mac::Gestalt.3pm.html](http://developer.apple.com/documentation/Darwin/Reference/Manpages/man3/Mac::Gestalt.3pm.html)

* if not using the best practice, writing applications that depend on a

third point of the OS version;

* if detecting a minor OS version, writing applications that

refuse to run
instead of displaying a warning dialogue.

Having said which, the definition of `MAC_OS_X_VERSION_ACTUAL`
does seem
incredibly short-sighted.

✦ Search Engine Dispute Notification (Re: Weinstein, [RISKS-24.72](#))

<"Kirakowski, Jurek" <jzk@ucc.ie>>
Wed, 20 Jun 2007 13:24:22 +0100

To see if I understand Lauren Weinstein's premise correctly, let me give an example: my company has a web site [A] on which we advertise a particular product that we have created and sell. A competitor sets up a web site [B] hosted in some odd place which gets either more, or round about the same number of, hits on a search engine when someone seeks information on distinctive keywords to do with my site [A]. This competitor's web site [B] contains derogatory, possibly misleading, and certainly unflattering information about my company and its product. It may even pretend to be my company and might sell a similar product or a clone of mine.

Search engines will as search engines do and [A] and [B] are likely to come close in keyword searches because that is the skill of [B] to be able to second-guess the algorithms.

Getting court orders against [B] will take ages, and may not be effective.

Lauren proposes that a 'dispute register' be set up in which [A] can register that [B] and [A] are in dispute about content. The entry in the register can't afford to make veracity claims or to take sides. It can only note that there is a dispute between [A] and [B], which dispute has been notified to the register by either owners of [A], [B] or both. If there is an attempt by the register to make veracity claims, then a clever faker of site [B] could tie up a process indefinitely with specious arguments (and oh boy, have we all heard some lulus!)

The best way for the register to work is that if a searcher finds either [A] or [B] they will also be given a link to the entry in the register.

However, if the searcher has to go to a special list at, say, disputes.org then if I were [B] I would certainly want to draw the searcher's attention to the entry in this list and rely on my ability to scam. If I were [A] it would not matter: someone has already found my site [A] and I would either warn the searcher of counterfeit sites, or present my information in such a way that it would be convincing.

Either way, this makes the job of [B] even easier. All [B] has to do now is to set up a bogus site, never mind the keywords or any expertise in getting noticed by a search engine. Having set up his misleading site, he then notifies the register that [A] and [B] are in dispute as if he were the aggrieved party.

And so even if it works for a small percentage of searchers, [B] has made his hit.

The only real cure is web savvy and siting oneself within web communities.

It may take a while for this to sink in (how many people STILL get caught in

'Lotto' scams?), but on the web where there is a lot of free information the

seeker should understand that the rule CAVEAT EMPTOR applies.

Let the buyer

beware.

My best defence as [A] is as follows:

I contact sites which reference mine [C],[D]... and ask them to put a note

next to their listing of [A] saying something to the effect that the reader

should be aware that bogus sites have appeared (not giving their URLs!) A

person browsing for the distinctive keywords of my site will likely find

mention of my site on other sites indexed by the same keywords [C], [D]...

and will find this information. This is not a route available to the bogus

site owner [B] who does not have the same peer network as I do.

It will be

in the best interests of [C], [D]... to assist me in this as they themselves

may one day come under attack in this way.

If someone browses using the distinctive keywords they will get [A], [B],

[C], [D]... and will see that there is a problem between [A] and [B].

I offer this more in the spirit of a 'straw man' since there must be an

obvious rejoinder which unfortunately this morning I just can't

see.

✦ Exploiting Online Games, Hوجلund/McGraw

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

Sun, 15 Jul 2007 13:32:35 PDT

Greg Hوجلund and Gary McGraw
Exploiting Online Games:
Cheating Massively Distributed Systems
(with a foreword by Ed Felten)
<http://exploitingonlinegames.com>,

<http://www.cigital.com/silverbullet/>
provides some background on the book.

Gary McGraw wrote:

The most interesting thing to me about EOG is that I believe the kinds of time and state errors found in MMORPGs [massively multiplayer online role-playing games] like World of Warcraft are indicators of what we can expect over the next decade as SOA actually catches on. You see, moving around state between gazillions of clients and a central server in real time is a huge security challenge. Most software people screw it up.

Darkreading wrote a little story about this:

http://www.darkreading.com/document.asp?doc_id=128961&WT.svl=news1_1

The book is packed with real code, hard-core examples, and things you can try yourself. Give it a spin!

For multiplayer game developers, the book is a goldmine on virtual-world security -- particularly what needs to be learned from the RISKS Experience.

For RISKS readers not really interested in games per se, there is still much grist for the mill in this book. The subtitle of the book is perhaps the real hook, exploring what developers of large complex distributed systems need to learn and mistakes not to make. A quote from Avi Rubin is pithy:

"Every White Hat should read it. It's their only hope of staying only one step behind the bad guys." 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

Search RISKS using [swish-e](#)

Volume 24: Issue 74

Thursday 19 July 2007

Contents

- ["Microsoft Copy Protection Cracked Again" and who's surprised?](#)
[Fred Reinke](#)
 - [Re: Microsoft protects me against ... Microsoft](#)
[Peter Mellor](#)
 - [Re: Space Shuttle uses 2-version programming](#)
[A. Marc Passy](#)
 - [N-version programming & low-probability events](#)
[Henry Baker](#)
 - [Re: Hurricane forecasting uncertainty](#)
[Jonathan Kamens](#)
 - [Re: Gripen: Risks of safety measures in military jet](#)
[Name withheld](#)
 - [Re: Search Engine Dispute Notification](#)
[Lauren Weinstein](#) [Nick Brown](#) [Paul Schreiber](#)
 - [Info on RISKS \(comp.risks\)](#)
-

➤ **"Microsoft Copy Protection Cracked Again" and who's surprised?**

<Fred Reinke <reinkefj@reinke.cc>>

Tue, 17 Jul 2007 14:32:42 -0400

Jessica Mintz, AP, 17 Jul 2007

Microsoft Copy Protection Cracked Again

http://www.breitbart.com/article.php?id=2007-07-17_D8QEFI301

<http://www.breitbart.com/article.php?id=2007-07-17_D8QEFI301&show_article=1&cat=breaking>

&show_article=1&cat=breaking

Microsoft Corp. is once again on the defensive against hackers after the

launch of a new program that gives average PC users tools to unlock

copy-protected digital music and movies.

The latest version of the FairUse4M program, which can crack Microsoft's

digital rights management system for Windows Media audio and video files,

was published online late Friday. In the past year, Microsoft plugged

holes exploited by two earlier versions of the program and filed a federal

lawsuit against its anonymous authors. Microsoft dropped the lawsuit after

failing to identify them.

The third version of FairUse4M has a simple drag-and-drop interface. PC

users can turn the protected music files they bought online—either a la

carte or as part of a subscription service like Napster—and turn them into

DRM-free tunes that can be copied and shared at will, or turned into MP3

files that can play on any type of digital music player.

Like an arms race, the DRM folks are spending a lot of cycles on a failing

paradigm.

Like putting lipstick on the proverbial pig, it annoys their paying customers and is pretty ugly! Some of my biggest irritations, in my computing career, have been at the hands of "copy protection". Couple that with bad, or non-existent, support and you have the seeds of a revolt.

I now don't buy content online -- music or other kinds -- if it has copy protection. I have a lot of expensive 8 tracks, cassettes, and cds of "content" that are unusable. Add to that "software", which has stopped working, stopped being supported, or otherwise orphaned.

My most recent experience was with MusicMatch JukeBox being acquired by Yahoo and forced to "upgrade". This was one of my last purchases, excuse me "licensing" -- what "barbara streisand"!! -- before my new policy of "no more".

"No more" locked content. "No more" buying software, excuse me licensing it, from vendors who are one step below used car salesmen. "No more" operating systems that require "activation" and have "self-help" provisions.

I look to the open source software makers and happily "donate" to their projects.

I'm calling out the content makers, "software" licensors, and the entire Microsoft empire as the hucksters they are. At least the snake oil sales men of yesteryear didn't try and make you "license" the bottle! A

plague on all
their houses.

Imagine how I'll be when I get old and crotchety!

Ferdinand J. Reinke, Kendall Park, NJ 08824 <http://www.reinke.cc/>

blog <http://www.reinkefaceslife.com/> <http://www.reinkefaceslife.com/>

Re: Microsoft protects me against ... Microsoft ([RISKS-24.73](#))

<MellorPeter@aol.com>

Tue, 17 Jul 2007 21:40:07 EDT

On 17 Jan 2007 I suffered a very similar incident. I had accepted Microsoft's regular automatic updates to Windows XP without problem for some time. On this occasion, it did a massive update taking over an hour, and I saw that my system had been upgraded from Service Pack 1 (SP1) to SP2. When I rebooted as instructed so that the upgrade could take effect, the reboot failed.

To overcome this I had to re-install Windows XP at SP1 level from the issue disk, and then recover various other facilities such as my broadband wireless connection. It took me until the end of January before I had a satisfactorily working system again (at SP1).

I have disabled automatic updating.

I kept detailed notes of the problem and how I overcame it, in

case anyone
is interested in a blow-by-blow account.

Peter Mellor; Mobile: 07914 045072; email: MellorPeter@aol.
com
Telephone and Fax: +44 (0)20 8459 7669

✈ Re: Space Shuttle uses 2-version programming (PGN, [RISKS-24.73](#))

<"A. Marc Passy" <marc.public@passy.us>>
Wed, 18 Jul 2007 09:32:59 -0500

> PGN: As I understand it, the following is true: the FIFTH
> computer is not
> fully functional -- it is intended to have just enough
programming to land
> the shuttle in the event that the four main computers all
fail. Testing
> it safely under live conditions where the first four computers
are
> inoperable is essentially undesirable, if not practically
impossible. The
> fifth system has never been invoked.

Mostly true, but it has been tested extensively in simulation.
(It actually
has both Ascent & entry functions - just no orbital functions.
It can get
you to orbit, just not do anything there but bring you home.)

> PGN: "Worse yet, it has most likely not been maintained for
compatibility
> with the other four. "

This is Flat Wrong. EVERY change to Shuttle software is
evaluated for both
PASS (primary Software) and BFS (Backup) impacts. It is

maintained to
EXACTLY the same standards as the PASS. (Though now, by just a
different
workgroup, not a whole different company.)

Marc Passy, Former NASA Flight Controller

[Marc, TNX for that. I appreciate your expert view. However,
"tested
extensively in simulation" strikes my formal-methods funny-
bone rather
oddly, given all the risks of what might be called `proof by
simulation'.
But I am glad to hear that PASS/BFS incompatibilities are not
a problem.
PGN]

⚡ N-version programming & low-probability events

<Henry Baker <hbaker1@pipeline.com>>

Thu, 19 Jul 2007 09:08:08 -0700

I've seen too many people dismiss errors that occur only once in
 10^9 or
even in 10^{12} events. These seem like very small probabilities,
which most
people would suggest are acceptable error rates. However, with
today's
video files growing to 100 or 1000 gigabytes (hidef 10 MByte/sec
for 10,000
secs = 100 GBytes), we now are facing even chances of errors *on
every
single video file*. If such an error occurs in the portion of
the file
which indicates its structure, one can easily lose substantial
fractions of
the entire file.

Another way to think about this problem is the following thought

experiment,
which was prompted by the "branch prediction" capability of
today's
microprocessors. Program a loop to execute 10^{12} times, which
is feasible
on today's processors. Since the probability of exiting the
loop is 10^{-12} ,
and therefore negligible, we can dispense with the exit test
entirely and
replace the loop with an infinite loop. QED

Re: Hurricane forecasting uncertainty (Gresko, [RISKS-24.69](#))

<Jonathan Kamens <jik@kamens.brookline.ma.us>>

Tuesday, July 10, 2007 9:03 AM

> The National Oceanic and Atmospheric Administration chief has
said written
> that the anticipated failure of QuikScat ("an aging weather
satellite
> crucial to accurate predictions on the intensity and path of
hurricanes",
> launched in 1999 and designed to last only a few years) could
add
> uncertainty to forecasts and broaden the areas over which
hurricane
> warnings and watches would have to be invoked.

For the record, Bill Proenza, the "chief" referred to above, has
now been
replaced, in no small part because of his public statements
about the
QuickScat risk.

Much of the staff at the NOAA's hurricane center disagreed with
Proenza
about the risk, and they were concerned that his the-sky-is-
falling message

might prompt Congress not to budget more money to replace QuickScat, but rather to take money from other parts of the NOAA budget which the staff felt were more important.

They first attempted to air their concerns privately. When that failed to have any effect, they published a letter, signed by 23 of the center's 50 employees, demanding his ouster. A quote from the letter: "The center needs a new director, and, with the heart of the hurricane season fast approaching, urges the Department of Commerce to make this happen as quickly as possible. The effective functioning of the National Hurricane Center is at stake."

Jonathan Kamens, IT Manager / Principal Engineer, Tamale Software
320 Congress Street, Boston, MA 02210 1-617-261-0264 ext. 133

✉ Re: Gripen: Risks of safety measures in military jet (Mellor, [R-24.73](#))

<Name withheld by request>

Wed, 18 Jul 2007 16:02:44 +0100 (BST)

> "Perhaps someone familiar with the Eurofighter could supply some
> authoritative information"

Eurofighter Typhoon has no automatic initiation of the Escape System other than linking the front and rear cockpits in the two seat variant, but even in this case the escape system has to be initiated by the aircrew.

Regarding the initiation of the escape system in Gripen allegedly by the anti-g suit, I find this highly unlikely. The Gripen uses the Martin-Baker Mk10 ejection seat, you can see some details here: <http://www.martin-baker.com/Products/Ejection-Seats/Mk--10.aspx>

The picture clearly shows the firing handle. In order to initiate the ejection the handle must be pulled to release it from its retaining bracket; on the Mk10 seat this will require a force of at least 15 pounds and then the handle must be pulled further (probably around one inch) whilst maintaining a force of at least 15 pounds.

You can see that the seat firing handle sits very close to what Monty Python referred to as "the naughty bits". Inflation of the anti-g trousers, if they contact the firing handle, is likely to impart force on either side of the handle in a sideways direction but none (or very little) in the upwards direction that is necessary to fire the system.

The handle itself is flexible and can be deformed; it's like stiff wire, so if the anti-g suit is responsible then it must impart at least 15 pounds of force upwards after deforming the handle and move the handle at least one inch. Something which I really can't see happening.

Typhoon uses the Martin-Baker Mk16A seat which, in terms of how the aircrew operate the escape system, is very similar to the Mk10 except that at least 30 pounds of force is needed to lift the handle.

To date there have been no un-commanded ejections from Typhoon.

Interestingly enough, looking at the Martin-Baker web-site the F35 Lightning II (JSF) uses a Mk16E seat which does have an auto initiate capability though I have no idea what conditions would activate this.

✉ **Re: Search Engine Dispute Notification (Kirakowski, [R-24.73](#))**

<Lauren Weinstein <lauren@vortex.com>>
Tue, 17 Jul 2007 13:09:22 -0700 (PDT)

Jurik apparently misunderstood a key premise in my public thinking on this subject, e.g.:

<http://lauren.vortex.com/archive/000253.html>

<http://lauren.vortex.com/archive/000254.html>

In particular, I have **not** suggested an "on-demand" system for search engine results dispute notifications.

Rather:

a) First line application would always be the legal system.

b) A third-party "independent entity" -- whether a formal organization or a distributed, virtual construct, would evaluate disputes that could not be directed to the legal system.

c) Only **very serious** attacks -- mainly against individuals (at the level of defamation, for example) -- would be considered for dispute link resolution.

d) Displayed dispute links would be ignored for the purposes of search

engine page ranking calculations.

e) Dispute links would simply point to a location for more information about

the particular situation -- they would not themselves provide detailed

information about the dispute.

In other words, this would definitely not be an "on demand" system.

Fundamentally, I want to make sure that there is recourse for people like a

woman featured on CNN recently. She has been mercilessly harassed by a

fellow with vicious false Web pages. She obtained a court judgment against

him, but he fled the country and his sites are now beyond the reach of a

U.S. takedown order.

Naturally, search engines continue to steer traffic to his defaming sites,

without any indication that something could be "wrong" about those pages, or

that a U.S. court has ruled against them. The damage to the targeted woman

continues.

I am unwilling to accept the concept that there must be no mechanism to warn

of very serious disputes, simply because there are many disputes that do not

rise to the level appropriate for such dispute link notifications.

Lauren Weinstein lauren@vortex.com or lauren@pfir.org +1 (818) 225-2800

<http://www.pfir.org/lauren> <http://www.pfir.org> <http://lauren.vortex.com>

Re: Search Engine Dispute Notification (Kirakowski, [RISKS-24.73](#))

<"BROWN Nick" <Nick.BROWN@coe.int>>

Wed, 18 Jul 2007 14:56:58 +0200

> I offer this more in the spirit of a 'straw man' since there
must be an
> obvious rejoinder which unfortunately this morning I just
can't see.

Allow me to try :-)

> This is not a route available to the bogus site owner [B] who
does not
> have the same peer network as I do.

I suspect that, since she is prepared to spoof your site, she is
probably
also prepared to contact C and D - or rather, the interns or
minimum-wager
McJobbers who maintain C and D's links pages - probably even
before you
notice that B is spoofing you.

(By getting her retaliation in first, she will have established
a useful bit
of psychological legitimacy too. A few years ago, some friends
of mine had
problems with noisy, antisocial neighbours. The first thing the
neighbours
did when they moved into their house - before turning up the
volume on the
hi-fi, banging on the walls, etc - was to call the police and
complain that
their neighbours (my friends) were harassing them from day one.
As a
result, it took months and several independent depositions

(fortunately,
there were other neighbours) before it was realised who were the
real
troublemakers.)

> It will be in the best interests of [C], [D]... to assist me
in this as
> they themselves may one day come under attack in this way.

In addition to the "intern" consideration above, this also
assumes that the
people who make policy at C and D have the time and the
inclination to make
the world a better place by signing up to a social movement
which promises
them some potential future benefit, without any guarantees. I
suspect that
this will not find much space in their timetable between the
modern Holy
Trinity (budget, deadline, and quality plan).

Nick Brown, Strasbourg, France.

⚡ **Re: Search Engine Dispute Notifications (Cowan, [RISKS-24.71](#))**

<Paul Schreiber <shrub@mac.com>>

Thu, 5 Jul 2007 10:05:19 -0700

> ... individuals who feel defamed by slanderous web sites just
need to
> copyright or otherwise classify that information about
themselves as
> intellectual property, and then issue a DMCA take-down
order. :-)

I know this was intended as a joke, but Crispin get the details
wrong, make it
slightly less funny and muddying an already confusing issue.

* You can't copyright "information about themselves" Facts are not copyrightable. You can only copyright something fixed in material form. If you had written something and they had copied it verbatim, that *might* be infringing.

* "or otherwise classify...as intellectual property" The DMCA only applies to copyrighted works, not to trademarked or patented items.

As for the real world, well, you could probably get away with it, because experience shows DMCA take-down notices are rarely verified.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 75

Wednesday 25 July 2007

Contents

- [Thompson, Langevin Release GAO Cybercrime Report, Announce Plans to Improve Private Sector Cybersecurity](#)
[CHSMajorityPress](#)
- [Vista Mail claims rejected mail has been sent](#)
[Neil Youngman](#)
- [SAIC sent military medical data unencrypted via the Internet](#)
[PGN](#)
- [Whoops! Nevada governor accidentally posts Outlook password](#)
[Declan McCullagh](#)
- [Wimbledon and the space shuttle](#)
[Mike Scott](#)
- [iPhone security flaw](#)
[Chris Leeson](#)
- [Right to Interfere with eBay Auctions](#)
[Greg Beck via Monty Solomon](#)
- [NTSB report pending on Comair Flight 5191 crash in Lexington KY](#)
[PGN](#)
- [IT risks in the Chemical Facility Anti-Terrorism Standard?](#)

[David E. Price](#)

● [Risks: Cellular carrier account security](#)

[Gabe Goldberg](#)

● [Risks of purism](#)

[Tim Panton](#)

● [Re: Space Shuttle uses 2-version programming](#)

[Robert Woodhead](#)

● [Re: Gripen: Risks of safety measures in military jet](#)

[Urban Fredriksson Claes T Nani Isobel](#)

● [REVIEW: "Backup and Recovery", W. Curtis Preston](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ Thompson, Langevin Release GAO Cybercrime Report, Announce Plans to

<CHSMajorityPress <CHSMajorityPress@mail.house.gov>>

Mon Jul 23 10:48:59 2007

Improve Private Sector Cybersecurity

Thompson, Langevin Release GAO Cybercrime Report, Announce Plans to Improve Private Sector Cybersecurity

July 23, 2007 (WASHINGTON) - Today, Congressman Bennie G. Thompson (D-MS), Chairman of the Committee on Homeland Security, and Congressman James R. Langevin (D-RI), Chairman of the Subcommittee on Emerging Threats, Cybersecurity, Science and Technology released a report conducted by the Government Accountability Office (GAO) on public and private challenges in addressing cybercrime.

The GAO reaffirms the threat that cybercrime poses to U.S.

national and economic security interests. In 2005, the Federal Bureau of Investigation estimated American businesses lost \$67.2 billion due to computer crime. Threats come both from at home and abroad; though many cyberattacks originate on U.S. soil, foreign adversaries continue to make public statements about exploiting vulnerabilities in technology to their advantage.

According to the GAO, the public and private sectors face numerous challenges to secure cyberspace, both in operational security and in law enforcement. Both public and private sectors have run into difficulties detecting or reporting cybercrime; the sectors have struggled to implement strong information security programs; there is a lack of adequate law enforcement analytical and technical capabilities to confront these challenges; and the borderless environment of cybersecurity makes it difficult for law enforcement to hold accountable those who break laws.

Chairman Thompson issued the following statement regarding the findings:

"When it comes to cyber, we have two worlds to secure - the public and the private sector. In order to provide leadership to the private sector, the Department of Homeland Security must demonstrate control of its networks. Unfortunately, previous GAO engagements and our own investigations into the Department have shown that 'information security' has become an oxymoron.

This is simply unacceptable. This Administration and the Department's leadership may continue to disregard these problems, but this Committee will continue to demand accountability from the government contractors and employees charged with securing information networks."

Chairman Langevin added:

"I encourage all businesses - small and large - to take a very close look at their cybersecurity practices. Though 100% security may be unattainable, there are many policies and procedures that businesses can implement to better safeguard their data.

Just as the government must improve its cybersecurity posture, so too must the private sector. The private sector is the nation's economic engine and the owner of a great majority of the national critical infrastructure. American businesses must come to realize that the security of the information that they keep is as important as the bottom line. In the upcoming months, this Committee will lead the conversation about ways to spur private sector investment in cybersecurity. Recently, Assistant Secretary for Cybersecurity and Telecommunications Greg Garcia asked us to consider legislation to help make the case for private investment. In addition to our efforts designed to improve Federal network security, I will work with Chairman Thompson to identify plans for incentives and liabilities that will improve private sector cybersecurity."

FOR MORE INFORMATION:

Please contact Dena Graziano or Todd Levett at (202) 225-9978.

United States House of Representatives
Committee on Homeland Security
H2-176, Ford House Office Building, Washington, D.C. 20515
Phone: (202) 226-2616 | Fax: (202) 226-4499
<<http://homeland.house.gov/>>

✶ Vista Mail claims rejected mail has been sent

<"Neil Youngman" <Neil.Youngman@wirefast.com>>
Fri, 20 Jul 2007 09:24:27 +0100

Here's a nice little problem with "Vista Mail". It appears that in some circumstances a "550" permanent rejection SMTP response is ignored and Vista Mail shows the mail as haven't been sent, even though the mail server rejected it.

<http://lists.exim.org/lurker/message/20070718.140135.4765aa65.en.html>

The reason seems to be that Vista mail can't handle multiline responses correctly.

<http://lists.exim.org/lurker/message/20070719.161335.f220a4a6.en.html>

The risks of MS being unable to implement a simple protocol correctly are obvious.

Neil Youngman, Developer, Wirefast Limited +44 (0)20 7592 1258

✦ SAIC sent military medical data unencrypted via the Internet

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

Sat, 21 Jul 2007 17:54:17 PDT

Air Force investigators are probing a security breach at Science Applications International Corp. (SAIC) of San Diego, which handles sensitive health information for 867,000 U.S. service members and their families. SAIC has acknowledged that some of its employees sent data over the Internet unencrypted, including medical appointments, treatments, and diagnoses. Two years ago, SAIC had a computer intrusion that resulted in the leakage of SSNs and other personal info on tens of thousands of its employees -- including former SAIC executive David A. Kay, who was the chief U.N. weapons inspector in Iraq, and a former director who was a top CIA official. [Source: Ellen Nakashima and Renae Merle, Military Medical Breach Revealed: Unencrypted Data Sent Via Internet, *The Washington Post*, 21 Jul 2007, D01; PGN-ed]

<http://www.washingtonpost.com/wp-dyn/content/article/2007/07/20/AR2007072001422.html?hpid=sec-health>

✦ Whoops! Nevada governor accidentally posts Outlook password

<Declan McCullagh <declan@well.com>>

Fri, 20 Jul 2007 11:25:41 -0700

[The files have been deleted since my story went up, but, unfortunately

for the governor's office, are still available on Google's cache:

<http://www.google.com/search?q=site%3Alistserv.nv.gov>]

Declan McCullagh [via Politech distribution],
Nevada governor accidentally posts Outlook password, 20 Jul 2007
http://news.com.com/8301-10784_3-9747705-7.html

If you ever wanted to be Nevada's governor for a day, it doesn't seem to be that hard.

In what could be a whopping security hole, Nevada has posted the password to the gubernatorial e-mail account on its official state Web site. It appears in a Microsoft Word file giving step-by-step instructions on how aides should send out the governor's weekly e-mail updates, which has, as a second file shows, 13,105 subscribers.

The Outlook username is, by the way, "governor" and the password is "kennyc". We should note at this point that the former Nevada governor, a Republican, is Kenny C. Guinn, which hardly says much about password security. [...]

Archived at <http://www.politechbot.com/>

Wimbledon and the space shuttle

<Mike Scott <usenet.10@scotts.dnsalias.com>>

Fri, 20 Jul 2007 10:31:11 +0100

Not a lot to do with each other, one might have thought. But PGN's comment in [RISKS-24.74](#) about "proof by simulation" struck a chord.

I'm referring particularly to this year's Wimbledon tennis tournament. For some years, the BBC has used simulations to show a virtual image of the ball's path, and in particular where it has bounced. I've wondered periodically how accurate these were - presumably /something/ has to track the ball in real time and model its trajectory. I've no idea how it's done. What I /do/ remember from the last year or so is that the Beeb once played back in close succession both a real video replay close-up of the ball bouncing, and then the simulation: it was quite clear that the simulation was at least 2 or 3 inches adrift, more than enough to make the difference between a line call being 'in' or 'out'

This year, they actually relied on Hawkeye [the simulator] as final arbiter in line calls - an umpire refused to over-rule it on at least one occasion. Separately, a BBC commentator said something like, "if we question Hawkeye, whatever next?". One of the finalists, IIRC, went so far as to question the system's accuracy however. Interestingly, the BBC used a lot of Hawkeye simulation replays to show the bounce of the ball - but I don't recall seeing a single close-up /video/ replay of the bounce this year.

Of course, tennis line calls are notoriously difficult, and Hawkeye may be more accurate overall than people's judgment; nevertheless, the blind faith

in it is worrying. Hawkeye at least has the benefit that it can't be intimidated by the "brats" of the game :-)

[There were several Hawkeye simulations that seemed obviously wrong to the commentators, spectators, and TV viewers. RISKS has often warned about people overendowing the infallibility of technology. Despite being steeped in old traditions, Wimbledon seems to be the latest victim. PGN]

iPhone security flaw

<"Chris Leeson" <Chris.Leeson@atosorigin.com>>

Tue, 24 Jul 2007 09:18:43 +0100

I suppose it was inevitable - someone has found a security vulnerability in the iPhone:

Dan Goodin, "Jesus Phone" needs an exorcist; security flaw means demonic

possession for Apple iPhone, *The Register*, 24 Jul 2007

<http://www.theregister.co.uk/2007/07/24/>

[iphone_security_vulnerability/](http://www.theregister.co.uk/2007/07/24/iphone_security_vulnerability/)

If a person visits a malicious website, then the phone can be infected with malware. Not a direct attack (in other words, launchable from the person sitting next to you), but I expect that is coming...

I remember the days when the only thing you could do with a mobile phone was ring people...

⚡ Right to Interfere with eBay Auctions (Greg Beck)

<Monty Solomon <monty@roscom.com>>

Fri, 20 Jul 2007 16:05:03 -0400

Companies Claim Right to Interfere with eBay Auctions for
Charging Too Little

Greg Beck, 17 Jul 2007

<http://pubcit.typepad.com/clpblog/2007/07/leegin-and-ebay.html>

I predicted that companies would soon rely on the Supreme Court's decision in Leegin Creative Leather Products v. PSKS to justify interfering with competition from less expensive products sold online. It did not take long for that prediction to come true. Although interference with eBay sales is nothing new, companies in two recently filed federal cases explicitly invoke Leegin as a justification for terminating the eBay auctions of competitors that charge lower prices online. These cases not only show Leegin's likely effect on Internet sales, but are also, unfortunately, fairly typical examples of the sort of anticompetitive actions companies take to fight lower-priced competition online.

⚡ NTSB report pending on Comair Flight 5191 crash in Lexington KY

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

Mon, 23 Jul 2007 10:30:12 PDT

Comair pilot instructors testified that the crew of Comair Flight 5191 committed numerous procedural violations relating to briefing, taxiing, and "sterile cockpit" rules (maintaining a distraction-free cockpit) before taking off from the wrong runway and crashing near the Lexington KY airport 27 Aug 2006, killing 49 people (see [RISKS-24.41](#)). Their testimony is apparently consistent with evidence released by the NTSB showing that the pilots violated company and Federal Aviation Administration rules by talking about their families, work and other subjects while preparing for takeoff. However, Comair maintains pilots were "confronted with inaccurate and inadequate airport charts, maps, signs, barriers, markings, and lighting". [Source: *Lexington Herald-Leader*, 23 Jul 2007; PGN-ed. Also, only one air traffic controller was on duty ([RISKS-24.43](#)).] <http://www.kentucky.com/471/story/127516.html>

⚡ IT risks in the Chemical Facility Anti-Terrorism Standard?

<"David E. Price, SRO, CHMM" <price16@llnl.gov>>
Wed, 25 Jul 2007 09:59:44 -0700

I was looking at the recent interim Chemical Facility Anti-Terrorism Standards, 6CFR27, while preparing a briefing on audit possibilities.

The Standard contains the following provisions:

27.230 (a) (7) Sabotage. Deter insider sabotage;

27.255 (d) Records required by this section may be kept in electronic

format. If kept in an electronic format, they must be protected against

unauthorized access, deletion, destruction, amendment, and disclosure.

These requirements seem pretty straightforward. However, there is a risk in counting on regulators to fully think through requirements such as these.

How can a facility protect electronic records from deletion, destruction, or amendment by disgruntled insiders such as management, IT personnel, security personnel, or onsite fire-fighters who all have access to the rooms housing the electronic equipment?

Two server rooms with separate IT staff could work for the IT group and possibly management, but it likely isn't feasible to block access to security or first response personnel. (I once worked as an Operations Supervisor at a commercial nuclear plant. Management decided that a block of offices contained material too sensitive to allow the fire brigade access after hours. A smoldering trash can which convinced us to break down a door in the middle of the night quickly pointed out the flaw in that thinking, and we got keys the next day.)

The only easy (partial) solution I could think of involves offsite storage, with the storage company personnel having read-only access to the onsite records and onsite staff having read-only access to the offsite

files. However this only reduces but doesn't eliminate the risk, especially for alteration. (The offsite backup would likely mirror any unauthorized onsite alteration. This seems to call for incremental backups with retention of all versions.)

And of course the offsite backup solution increases the risk of disclosure.

Maybe the key is in the requirement to deter and protect rather than prevent insider sabotage, but this quickly turns into an audit nightmare of how much deterrence is enough.

⚡ Risks: Cellular carrier account security

<Gabe Goldberg <gabe@gabegold.com>>

Fri, 20 Jul 2007 22:51:36 -0400

When I established my cell phone account I saw no reason to provide my social security number, so I gave them random digits, which I then forgot. So I couldn't make account changes (since last four SSN digits are used for PIN!) no matter how I explained that they didn't have my real SSN so I couldn't tell them the what their screen displayed for my account. Today I called and simply said there was a problem with my account, the record had the wrong SSN, and I'd like to fix it. No problem, no identity verification, the rep happily accepted four new digits, which I then used on their Web site to update my account.

⚡ Risks of purism

<Tim Panton <thp@westhawk.co.uk>>

Fri, 20 Jul 2007 11:16:36 +0100

In [RISKS-24.74](#) PGN rightly casts doubt on the validity of 'proof by simulation'.

I'm a fan of well designed simulations. In a former life I was involved in the testing of a control system for a chemical plant.

We created a faithful simulation of the plant, then arranged for our simulator to output voltages that mimicked the sensors that were in the real plant. We then plugged these outputs into the control system and went through a series of tests.

The results were totally unexpected. It failed, in some cases the simulated plant responded too slowly. We assumed that the problem was the simulation or the interfaces. After much study we concluded it wasn't. The control system was at fault, and in a subtle way, the control blocks covering the most time critical loops had been spread over multiple processors and the inter-processor communication was introducing a significant delay. The manufacturer 're-optimized' the loops and the problem was fixed.

Used appropriately simulations (or stimulations ?) can tell you things you couldn't easily find any other way, so should be in the toolbox

of any
serious tester.

✶ **Re: Space Shuttle uses 2-version programming (PGN, [RISKS-24.74](#))**

<Robert Woodhead <trebor@animeigo.com>>

Fri, 20 Jul 2007 09:41:28 +0900

Consider the risks of live-testing the backup software. If it has a bug, you've potentially lost a shuttle and crew. Brings a whole new meaning to "live testing", doesn't it?

Since the backup software isn't going to ever be used until after the fecal matter has hit the rotary impeller at high velocity (does the shuttle toilet have a rotary impeller? IIRC it does...), not testing it under live conditions may well be the lower-risk path. Sometimes the risks of testing outweigh the benefits.

[Added note: Well, I was struck by the meta-risk. Or maybe it's better classed as a "reentrant risk" (smirk). RW]

✶ **Re: Gripen: Risks of safety measures in military jet**

<Urban Fredriksson <griffon@canit.se>>

Fri, 20 Jul 2007 09:16:40 +0200 (MET DST)

"The picture clearly shows the firing handle." Yes, of a Mk.10LH seat. It looks different on a Mk.10LS seat as can be seen here: <http://www.canit.se/%7Egriffon/aviation/img/ljungbyhed96/mbmk10.jpg>

Photo shows a A/B version seat, the C/D was given a stiffer handle. Saab says they were able to duplicate the initiation using test subjects with large thighs, the temporary fix was to restrict flying to 3G and the air force has said the permanent fix is to fit more flexible handles. Doesn't seem like there's any doubt as to what happened although the official investigation is still listed as ongoing.

✶ **Re: Gripen: Risks of safety measures in military jet ([R-24.74](#))**

<Claes T <claes.t@nejtillspam.se>>

Fri, 20 Jul 2007 12:08:23 +0200

[seat firing handle]

>The handle itself is flexible and can be deformed; it's like stiff wire, so
>if the anti-g suit is responsible then it must impart at least 15 pounds of
>force upwards after deforming the handle and move the handle at least one
>inch. Something which I really can't see happening.

>Typhoon uses the Martin-Baker Mk16A seat

Please note the handle has been changed in the Gripen C/D-versions: the

"wire" is replaced with a heart-formed ring on a short stick.

So, the Typhoon comparison isn't relevant. A picture of the handle versions can be found at <http://www.nyteknik.se/art/51034> [text in Swedish only]. A SAAB spokesman says in the article (from June 5th) the handle has been found slightly pushed upwards and not always full retracted after repeated occasions of high G-load in performed tests after the crash, and that all handles now should be replaced with a more soft handle like the one in earlier Gripen versions.

⚡ **Re: Gripen: Risks of safety measures in military jet ([R-24.74](#))**

<Nani Isobel>

Mon, 23 Jul 2007 23:58:06 -0500

There may be a way the ejection handle can get pulled. Start with a high-g turn, pitch up, causing the suit to inflate and grip the handle. Follow it with a high-g turn, pitch down, causing the pilot to be pulled up into the belts while the suit is still inflated. If the belts are loose or if they stretch, the pilot could move up by an inch.

⚡ **REVIEW: "Backup and Recovery", W. Curtis Preston**

<Rob Slade <rMslade@shaw.ca>>

Mon, 23 Jul 2007 12:34:08 -0800

BKBAKREC.RVW 20070302

"Backup and Recovery", W. Curtis Preston, 2007, 0-596-10246-1,
U\$49.99/C\$64.99

%A W. Curtis Preston www.backupcentral.com
curtis@backupcentral.com

%C 103 Morris Street, Suite A, Sebastopol, CA 95472
%D 2007

%G 0-596-10246-1 978-0-596-10246-3

%I O'Reilly & Associates, Inc.

%O U\$49.99/C\$64.99 800-998-9938 fax: 707-829-0104 info@ora.com

%O <http://www.amazon.com/exec/obidos/ASIN/0596102461/>

[robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0596102461/robsladesinterne)

<http://www.amazon.co.uk/exec/obidos/ASIN/0596102461/>

[robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0596102461/robsladesinte-21)

%O <http://www.amazon.ca/exec/obidos/ASIN/0596102461/>

[robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0596102461/robsladesin03-20)

%O Audience a Tech 2 Writing 1 (see [revfaq.htm](#) for explanation)

%P 729 p.

%T "Backup and Recovery"

We tell people to make backups. Occasionally we might mention the difference between full, differential, and incremental backups. If we are turning out hotshot forensics specialists we might even go into the difference between file image backups and disk image backups. But how often do we tell people that operational databases (which is most of them) have open files, and generally prevent you from backing up with the usual utilities?

Part one is an introduction. Chapter one is an overview of some quick aspects about backups, but primarily is a suggestion to do it, and do it properly. Basic types of backups, and the factors affecting backup

procedures, are outlined in chapter two. (The material will probably feel very familiar to those who have worked in the business continuity field: not just because of the importance of backups in recovery operations, but also because of the analysis of the complex and interdependent linkages that can cause disasters.)

Part two examines open source backup utilities. (Most of them are open source: a few are just "free.") Chapter three reviews some of the utilities for UNIX, Linux, Windows, and the Mac that can provide fundamental backup capabilities, and which can also be used by other applications for more sophisticated backup systems. Amanda (the Advanced Maryland Automated Network Disk Archiver), an open source, cross-platform, client/server architecture (Windows servers do not appear to be available, but clients are) backup system that uses some of these underlying tools is described in chapter four. Amanda has some very interesting security and scheduling provisions. BackupPC, a network-based backup system for UNIX (client or server) and Windows (client) is briefly described in chapter five. Chapter six explains another distributed system, Bacula, in a rather haphazard manner. Rsnapshot, which does near-continuous backup, is delineated in chapter seven.

Part three supposedly turns to commercial backup products. In fact, the contents are simply a list of factors to be used when evaluating software products (chapter eight) and various types of hardware (nine).

Bare-metal recovery (what you do to restore the system when you've lost the whole thing, rather than just a few files) is described in part four. The Solaris flash archive is intended for cloning of systems, but chapter ten tells how to use it for recovery. Chapter eleven explains tools and procedures for Linux, and a little tiny bit for Windows as well. Procedures for HP-UX are in twelve, AIX in thirteen, and Mac OS X (which basically has a version of BSD under the graphical user interface) is in fourteen.

Database systems have a) lots and lots of data, b) special backup requirements, and c) a special importance to most companies, so this application gets special attention in part five. General concepts are discussed in chapter fifteen, with the particulars of backup and recovery for Oracle, Sybase, DB2, SQL Server, Microsoft's Exchange (well, an email server certainly *uses* a database ...), PostgreSQL, and MySQL in chapters sixteen to twenty-two.

Part six covers miscellaneous topics. Actually, it is chapter twenty-three that contains miscellaneous topics (starting out with how to back up VMWare servers). Chapter twenty-four is a justification for the book (or, for having a backup process, anyhow).

Preston's work is directed at inexpensive backup solutions for open systems, so it is not surprising that UNIX utilities get the most space and the greatest attention to detail. Windows is certainly not ignored, and the

author even bends his own rules to accommodate some helpful utilities in the Windows realm, but there simply isn't a lot of material to work with.

Backups are important for everyone. This book is not for everyone. The text will be very valuable for those who have large systems, or large numbers of systems, with backup needs complicated by special situations.

Now go make a backup.

copyright Robert M. Slade, 2007 BKBAKREC.RVW 20070302
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<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

Search RISKS using [swish-e](#)

Volume 24: Issue 76

Tuesday 31 July 2007

Contents

- [Scientists' Tests Hack Into Electronic Voting Machines](#)
- [California Voting System Hacking Report](#)
[Rebecca Mercuri](#) PGN
- [Earthquakes and O rings](#)
[Rod Van Meter](#)
- [If this guy's telling the truth, he should never fly an airplane](#)
[Erling Kristiansen](#)
- [Three little zeroes](#)
[Mark Brader](#)
- [Department of Health Proposes New Records System](#)
[EPIC News](#)
- [Comair Flight 5191](#)
[Andrew Koenig](#)
- [Re: Accuracy of Hawkeye at Wimbledon](#)
[David Alexander](#)
- [Re: iPhone Security Flaw](#)
[Nicholas Weaver](#)
- [Re: Risk with the Mac OS X 10.4.10 version number](#)

[Richard Grady](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ Scientists' Tests Hack Into Electronic Voting Machines

<Daniel Graifer <graifer@earthlink.net>>

Sat, 28 Jul 2007 13:30:35 -0400

"Computer scientists from California universities have hacked into three electronic voting systems used in California and elsewhere in the nation and found several ways in which vote totals could potentially be altered, according to reports released yesterday by the state."

The article includes discussion of the current House bill to require paper audit trails.

Source: *The New York Times*

<http://www.nytimes.com/2007/07/28/us/28vote.html>

Daniel A. Graifer Home: 703-425-4512 Cell: 703-967-3635

⚡ California Voting System Hacking Report

<"R. Mercuri" <notable@mindspring.com>>

Fri, 27 Jul 2007 20:14:59 -0400

Just in case you haven't seen this yet, here's the California Overview of the Hacking Report:

http://www.sos.ca.gov/elections/voting_systems/ttbr/

[red_overview.pdf](#)

My executive summary of the overview is as follows:

At a cost of \$1.8M, the California Secretary of State now has a report that confirms that all of the State's Hart, Diebold and Sequoia DRE and OpScan voting systems can be hacked in various ways. Potential hacks include the all-important ability to have a VVPAT print out one thing and the DRE total reflect something else, thus rendering the VVPAT moot, as well as the capability of detecting election mode (thus enabling the pre-election testing to appear correct, while the actual election has been compromised). All of these are types of hacks that many knowledgeable people have been saying for years could happen, and now we know that for sure they can. Oh, and guess what else? "The security mechanisms provided for all systems analyzed were inadequate to ensure accuracy and integrity of the election results." Gee, what a surprise.

Unfortunately the report provides a fall-back position whereby these wretched election products can continue to be used -- by claiming that many of the attack scenarios can be mitigated through better physical security, security training of staff, and contingency planning. Of course the report fails to mention that if the staff or the vendor is corrupt and their contingency plan is to cover up their tracks, we now know for sure that a game plan for fraud is certainly possible. So let's just throw more money at additional security mechanisms and training while we all pretend that we're

conducting legitimate elections. Good job, guys, thanks for letting the CA SoS off the hook.

Here's a novel thought: why not just throw this crap in the junk heap where it belongs, vote on paper, and let the citizens do the counting? Maybe for another \$1.8M some State can get a team of PhDs to validate that conclusion.

Rebecca Mercuri.

Permission Granted to Post This Message in its Entirety.

California Voting System Hacking Report

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

Apparently along with many other Web watchers, I spent time yesterday watching an all-day hearing of the California Secretary of State, Debra Bowen, interrupted by frozen screens presumably resulting from too many people trying to follow the live webcast. In my opinion, Secretary Bowen has consistently sought a better understanding of the integrity, accuracy, reliability, and survivability of the electronic voting systems that are in use in California -- or the lack thereof. (Several of us had testified in February 2006 for her California Senate Elections Committee, with my testimony on the relative merits of openness in voting systems available at <http://www.csl.sri.com/neumann/calsen06.pdf> .)

Five reports are now available on the California SoS website:

http://www.sos.ca.gov/elections/elections_vsr.htm

including the red-team overview, red-team analysis of Diebold, Hart, and Sequoia systems, as well as a detailed analysis of accessibility and

usability of the three systems -- conducted by Noel Runyan and Jim Tobias.

Further reports analyzing source code and documentation for each of the

three systems have not yet been released; according to the website, these

reports will be posted "as soon as the Secretary of State ensures the

reports do not inadvertently disclose security-sensitive information."

Here are my own personal comments. (NOTE: I was *not* a part of the

Top-to-Bottom Review [TTBR], and have not been privy to any inside

information.)

I applaud analyses that provide greater sunshine in the election process,

even if they can address only a part of the total system.

(Election system

vendors have typically hidden behind proprietary status of everything --

including not only the software but also the data formats, and even internal

voting data in disputed elections.) However, analyses must always be

considered in the context of the total system -- hardware, software,

procedures, users, the physical premises, and so on. Given various late

starts and the fixed termination date for all of the efforts that was

imposed by the hearing, the results available thus far seem worthy -- albeit

clearly not surprising to those of us (including Rebecca Mercuri) who have

been involved in seeking integrity in the election process for many years.

(My involvement goes back to the mid-1980s.) The systems have generally been known to be lacking in good software engineering practice, built-in security, and measures that might have obviated the need for extensive operational procedures. The findings of the University of California teams can provide further evidence of that to those people -- including lawmakers -- who have not previously been exposed to the innards.

The red-team overview report, which notes the need for procedural mitigations to overcome the existence of technological vulnerabilities,

tries to give some perspective to the public by pointing out that the

electronic voting systems are only one part of a larger process. Long-time

RISKS readers by now know how important it is to consider the results of the

process as a whole rather than looking only at the individual pieces in

isolation. Also, note that the overview does not say **all** flaws can be

overcome; it says that the reviewers believe **many** can be compensated for.

As Matt Bishop stated during the final question-and-answer session of

yesterday's public hearing, his personal opinion is that some flaws require

changes to the technology, rather than just procedural adjustments. (This

occurs about 6:41:00 into the streaming video, which can be found at

<http://www.calchannel.com>.) I have generally believed this to be true,

because people are fallible and not always able or willing to follow the

procedures. It seems to be especially important in elections, in which

human frailty needs to be avoided and where tamper-resistant and tamper-evident audit trails are essential.

There were of course critics in the hearing who believe that the technological study was lacking in reality: for example, it was inherently incomplete because only 3 of the 9 systems currently in use in California were included; it did not adequately address procedural issues, which might compensate for the security and privacy protection vulnerabilities that the TTBR was intended to identify; it failed to caveat the vulnerabilities with an assessment of the risks of exploitation of the vulnerabilities. (On the other hand, RISKS readers are familiar with our persistent warnings about the risks of flawed quantitative risk assessment.) One complaint was that the effort was a waste of time, because no malware was detected. (However, the study never attempted to look specifically for malware. I would presume that the software provided by the vendors was free of intentional malware, and furthermore, given the demonstrated vulnerabilities, installing malware would not be at all difficult -- either in the development process or subsequently!) Several election officials reported being completely happy with the electronic systems, and claimed that there have never been any problems. (But many would-be problems with DREs can be undetectable.)

All in all, I believe that Secretary Bowen's desire for a top-to-bottom review of the entire election process will benefit from a better understanding of the technological vulnerabilities -- even though they certainly represent just one piece of the overall puzzle.

🔥 Earthquakes and O rings (via Dave Farber's IP)

<Rod Van Meter <rdv@sfc.wide.ad.jp>>

July 23, 2007 2:44:58 AM EDT

[Another example of the globality of local risks... PGN]

By now everyone has heard of the M6.8 earthquake up in Niigata last week, a couple of hours north of Tokyo by shinkansen. Ten people were killed (all in their 70s and 80s, living in traditional-style houses with heavy ceramic tile roofs that collapsed), 6,000 homes and buildings destroyed, roads cracked and/or covered by landslides, a fault slip that came to the surface and displaced a section tens of kilometers long by something like a meter. Net effect was (if I recall) to push one plate 16cm north.

The biggest newsmaker has been the effect on the Tokyo Electric Power (TEPCO) nuclear plant, the largest in the world. Leaks of radioactive water, hundreds of barrels of radioactive waste tipped over (some broke open and leaked), etc. The most recent list of problems was 63 items long. Opposed to or in favor of nuclear power, TEPCO's slow response and misinformation are creating a firestorm here. The reactor itself was designed to withstand only a 6.5; regulations were already under revision to up that number, but weaker plants will be in use for

decades.

But you knew that, and I want to talk about piston rings, not nuclear power.

One small company in Niigata, Riken (no relation to the research lab with a similar English name, I'm sure) makes 60% of the piston O rings used by *all* of the car manufacturers in Japan. Their plant was badly damaged.

Japan's auto makers, of course, are famed for their "just in time" supply chain management. I know people who have worked for subcontractors, and the penalty for being late in supplying a critical part can easily exceed \$100,000 A DAY.

Toyota was forced to idle at least 27 plants, Daihatsu four, Honda and other manufacturers several each. Toyota is still shut down, as of this writing (Monday, a week after the quake), and has an output loss of 46,000 cars or more. I haven't seen a breakdown of the percentage intended for domestic consumption versus export.

One interesting part of the response is that the auto manufacturers sent teams of their idled workers to Niigata to help Riken clean up and get back in production. They were there helping by Thursday, despite the transportation disruption, general shortages of goods including water, food, and electricity, and risk of aftershocks.

One point and one question:

* A disaster it is, but a relatively local one, in a mid-level city where events rarely make the world news. And yet it will affect car prices around the world, no doubt. Just one more data point that the world's economy is one large web.

* Toyota is a very well-run company, but they let this happen to them with an important single-sourced part. How good is YOUR disaster plan, whether personal or corporate? How good are your suppliers' disaster plans, and their suppliers'?

IP Archives: <http://v2.listbox.com/member/archive/247/=now>

⚡ If this guy's telling the truth, he should never fly an airplane

<Erling Kristiansen <erling.kristiansen@xs4all.nl>>

Fri, 27 Jul 2007 20:44:09 +0200

ADS-B ROLLOUT IS ON THE WAY

Wilson Felder, director of the William J. Hughes Technical Center in

Atlantic City that is evaluating the system, told reporters that ADS-B is

something all pilots should want in their panels. He's flown with it

personally for about 60 hours in his Cessna 172 and seen its value

firsthand. "It's saved my life at least three times," he said.

<<http://www.avweb.com>> issue 13.30e

[Must be a pretty lousy pilot if he needs to have his life saved 3 times by

a new gadget in 60 hours of flight!]

⚡ Three little zeroes

<msb@vex.net (Mark Brader)>

Fri, 27 Jul 2007 13:57:50 -0400 (EDT)

Frank Van Buran is an accountant in New York. He had an Exxon Mobil credit card for his business, which was expiring. He asked for two copies of the new one. He got them -- and then 2,000 more. Which were left in boxes on his doorstep, where anyone could steal them, and which the company expected him to destroy (it took hours). Nothing seems to have been publicized as to what exactly went wrong, but how could it be anything but computer-related?

http://www.nydailynews.com/money/2007/07/26/2007-07-26_tomfuelery-1.html

Mark Brader, Toronto, msb@vex.net | "Volts are like proof" -- Steve Summit

⚡ Department of Health Proposes New Records System (EPIC Alert 14.15)

<EPIC News <alert@epic.org>>

Fri, 27 Jul 2007 18:09:36 -0400

[Excerpted from Volume 14.15, 27 Jul 2007. PGN]

E P I C A l e r t
Published by the
Electronic Privacy Information Center (EPIC)
Washington, D.C.
http://www.epic.org/alert/EPIC_Alert_14.15.html

Department of Health Proposes New Records System

On June 26, the Department of Health and Human Services (HHS) proposed to establish the National Disaster Medical System (NDMS) Patient Treatment and Tracking Records System. The goal of this new records system is to collect individual health data from people receiving medical care provided by NDMS. The NDMS is a joint effort between HHS, the Department of Defense, the Department of Homeland Security, and the Veteran's Administration to provide additional resources to supplement the public health and health care actions local and state governments provide during emergencies.

Under the proposal, all persons treated by NDMS medical staff may have their health data recorded and placed into a record system. This would include demographic information as well as data regarding patient diagnosis, treatment, and location. This data may be obtained from the individual patients, their physicians, or by access to the health records of patients.

The NDMS Patient Tracking System contains various "routine use" disclosures to all the federal agencies that share responsibility for evacuation and treatment of patients under NDMS in order to ensure the highest level of patient care possible. Routine use disclosures may also be made to

consultants, contractors, and grantees who may require access to the health records for business purposes related to the collection of the data.

Lastly, routine use disclosures will be made to state and federal agencies as necessary to establish the benefit entitlement of the patient or to help families locate evacuated family members.

The routine use disclosures contained within the NDMS Patient Tracking System raise some privacy concerns that EPIC addressed in comments submitted to HHS on July 26. In the comments, EPIC stated that HHS should build privacy protections into the system in order to ensure that patients receive quality emergency health care without having to sacrifice their medical privacy. EPIC also urged HHS to clearly define how the system of records notice will comport with the Health Insurance and Portability Act (HIPAA). Any proposed routine use disclosures that violate HIPAA provisions should not be included.

The NDMS Patient Tracking System collects data during emergency situations. Due to the extreme nature of these events, privacy and safety can easily be overlooked if they have not already been built into the system. EPIC urged HHS to consider the impact that the proposed routine use disclosures could have on victims of domestic violence, as well as other displaced individuals. After Hurricane Katrina, numerous evacuees faced instances of personal information abuse. For this reason, EPIC encourages the use of health data collected by the NDMS for patient treatment purposes only.

EPIC's Webpage on Hurricane Katrina and Identity Theft:

<http://www.epic.org/privacy/idtheft/katrina.html>

EPIC's Webpage on Domestic Violence and Privacy:

<http://www.epic.org/privacy/dv/>

EPIC's Comments on NDMS Patient Treatment and Tracking Records System (pdf):

http://www.epic.org/privacy/dv/ndsm_comments.pdf

Department of Health and Human Services System of Records Notice (June 26, 2007) (pdf):

<http://www.epic.org/redirect/hhs2707.html>

✈ **Comair Flight 5191 ([RISKS-24.75](#))**

<"Andrew Koenig" <ark@acm.org>>

Thu, 26 Jul 2007 09:26:52 -0400

The report in [RISKS 24.75](#) inadvertently pointed out an example of an organizational antipattern--a kind of behavior that appears on the surface to solve a problem but actually does the opposite.

The first sentence: "Comair pilot instructors testified that the crew of Comair Flight 5191 committed numerous procedural violations relating to briefing, taxiing, and 'sterile cockpit' rules (maintaining a distraction-free cockpit) before taking off from the wrong runway..."

The fallacy is "post hoc, ergo propter hoc." In other words, the crew violated procedures, then crashed; so it is tempting to assume

that the violation caused the crash--despite the other problems cited later in the article. From a bureaucrat's viewpoint, this assumption can then be used to make the procedures more restrictive, increase crew monitoring, etc., all without proving that the procedures are actually useful.

Of course it is possible that the procedural violations caused the crash. The antipattern--and one that is particularly tempting for bureaucratic organizations--is to assume without proof that they did so, perhaps because that assumption is the one that most benefits the organization.

✈ **Re: Accuracy of Hawkeye at Wimbledon**

<David Alexander <dave_ale@online.rednet.co.uk>>

Fri, 27 Jul 2007 23:17:11 +0100

I read the submission from Mike Scott, regarding the errors he recalls seeing in the Wimbledon tennis 'Hawkeye' line-call system last year and the reliance of the Lawn Tennis Association upon it this year.

Mr Scott makes no allowance for the upgrades to the system, and testing, that have taken place in the intervening 12 months. It would have been wrong to rely on the system in its debut year because it certainly had some accuracy issues. Those have now been largely resolved and the system was used with overall approval from almost everyone. It's not perfect, but it's now more accurate than the 'mark one eyeball' of the line

judges. There were only 4 days out of the whole tournament where the challenges by players against its performance were upheld more than 50% of the time, after reviewing the footage.

This system has now been adopted for all of the Grand Slam tournaments except France, which is a clay court surface.

David Alexander, Towcester, Northamptonshire, England

[Challenges "upheld more than 50% of the time?" That would be an intolerable error rate for many other situations, such as the Employment Eligibility Verification System or a terrorist watch list or automated face recognition, especially on a large scale. On the other hand, some tennis players are known to have completely lost their cool as a result of egregious line calls. One might think that the chair umpire would call a LET instead of letting a "definitive" simulation stand when the margin of error of the simulation may be much greater than the width of the actual ball suitably flattened by an overhead smash. PGN]

✉ **Re: iPhone Security Flaw (Leeson, [RISKS-24.75](#))**

<Nicholas Weaver <nweaver@ICSI.Berkeley.EDU>>
Wed, 25 Jul 2007 14:49:15 -0700

Given the ease of spoofing packets and the other games which can be played

on a wireless network, it wouldn't surprise me if the "person sitting next to you" could exploit this to infect your system, e.g., by quickly bursting a HTTP redirect (even before the remote site really completes the handshake and realizes something is wrong) and then carrying out the exploit through the redirected page.

⚡ Re: Risk with the Mac OS X 10.4.10 version number (Yip, [RISKS-24.72](#))

<Richard Grady <richard@richbonnie.com>>
Sun, 29 Jul 2007 19:30:33 -0700

Microsoft had an analogous problem when MS-DOS was introduced, way before the Windows system. They solved it with the SETVER command. This excerpt explains the purpose of SETVER:

Definition of: DOS Setver

An external command starting with DOS 5 that updates a version table

containing names of programs and the DOS version number they need to run

under. Programs may test version numbers and function differently as a

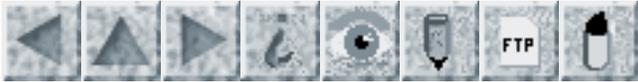
result (all DOS's are not the same), but some programs didn't plan on DOS

5 and DOS 6 as future numbers. This command "fakes them out" by supplying

them with the version number they need.

http://www.pcmag.com/encyclopedia_term/0,2542,t=DOS+Setver&i=41854,00.asp

Apple needs a version of the SETVER command.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 77

Friday 3 August 2007

Contents

- [Structural problems with the I-35W bridge span](#)
[PGN](#)
- [Driver follows GPS when he should not](#)
[Erwan David](#)
- ["Meteorology Police -- you're BUSTED!"](#)
[Annie Johnson via Paul Saffo](#)
- [Hacked passport crashes RFID readers](#)
[Jeff Jonas](#)
- [IRS computer security/privacy problems](#)
[PGN](#)
- [User-hostile behavior](#)
[Steve Summit](#)
- [Location-Based Dictionary Attacks](#)
[Diomidis Spinellis](#)
- [Amazon chasing 2-cent Web services bill](#)
[Martin Redington](#)
- [Windows Live Messenger blocking even more completely innocuous text](#)
[Cody Boisclair](#)

- [Re: Accuracy of Hawkeye at Wimbledon](#)
[Paul Wallich](#)
 - [Fraudproof voting protocols from scientists](#)
[Warren Smith](#)
 - [REVIEW: "Implementing ITIL", Randy A. Steinberg](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Structural problems with the I-35W bridge span

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

Thu, 2 Aug 2007 10:18:35 PDT

Two reports published since 2001 pointed to structural problems with the

Interstate 35W. ... The bridge's deck truss system has not experienced

fatigue cracking, but it has many poor fatigue details on the main truss

and the floor truss system. ... In another report two years ago, the

U.S. Department of Transportation's National Bridge Inventory database

concluded the bridge was "structurally deficient."

<http://www.cnn.com/2007/US/08/02/bridge.structure/index.html>

[noted by Mike Hogsett]

Bridges are generally built with a high level of redundancy, so that if

one part fails the load is distributed through the structure. The I-35W

bridge did not have a high level of redundancy, and the failure of a

single significant component could have led to the collapse of the entire

structure. [Annotation in A Deadly Collapse, a half-page set of graphics,

The New York Times, 3 Aug 2007, National Edition A14]

The propagating bridge structure collapse on 1 Aug 2007 in Minneapolis exposes just one more tip of an iceberg among a large collection of icebergs. Many of our infrastructures such as roads (some with sink-holes lying in wait), bridges, railroad track beds, pipelines, storage tanks (including fuel and nuclear waste), and so on are in serious need of repair, decommissioning, or replacement. For example, some of road infrastructures have endured loads far in excess of what was expected in their original designs and operating environments, and have been steadily declining. This is just another example of the old adage, "an ounce of prevention is worth a pound of cure". In this case, the scales are unbalanced by deaths that cannot be cured and collateral losses.

There is of course a lesson here for information system infrastructures, Removing information security vulnerabilities seems to be a nonstarter in the eyes of government and system developers that might otherwise stimulate remediation. The short-term costs of preventive maintenance always seem to blind folks to the long-term costs of inaction. This situation reminds me once again of the importance of farsighted design and continual oversight. See my two-page note on holistic systems in the November 2006 issue of the ACM SIGSOFT Software Engineering Notes, in case you have not looked at it yet:

<http://www.csl.sri.com/neumann/holistic.pdf>

I seem to have gone all these years of moderating RISKS without

citing one
of my favorite multipurpose mixed metaphors: Pandora's cat is
out of the
barn and the genie won't go back in the closet. It certainly
seems
applicable here.

⚡ **Driver follows GPS when he should not**

<Erwan David <erwan@rail.eu.org>>
Wed, 1 Aug 2007 14:21:43 +0200

On 22 Jul 2007, a Polish bus had a grave accident in Vizille
(France). The
bus used a road with a 14% (1/7) descending slope, it seems its
brakes went
too hot and could not stop the bus at the end of the slope.

The inquiry made appear that the driver blindly followed the
indications of
his GPS receiver, ignoring the 11 signs forbidding him to use
this route.

Risk: always relying on technology, even if used a little bit
out of spec.

⚡ **"Meteorology Police -- you're BUSTED!"**

<Paul Saffo <paul@saffo.com>>
Tue, 31 Jul 2007 16:40:45 -0700

A suspicious looking box found near Lewis-Gale Medical Center
[on 19 Jul
2007] was, in fact, a remote weather station that had been

affixed to a tree
by an employee, and not an explosive device. Constructed with
putty and
wires, it was probed by the Virginia State Police Bomb Squad --
which blew
it up before realizing it was a weather station. An employee
had placed a
putty-like substance around the box to make it weather
proof. ...

[Source: Annie Johnson, *The Roanoke Times*, 20 Jul 2007; PGN-
ed]

<http://www.roanoke.com/news/breaking/wb/125008>

⚡ Hacked passport crashes RFID readers

<Jeff Jonas <jeffj@panix.com>>

Wed, 1 Aug 2007 03:36:39 -0400 (EDT)

The report that voting machines are not trustworthy is joined by
this: RFID
passports and readers are vulnerable:

http://www.boingboing.net/2007/07/31/hacked_passport_cras.html

<http://www.wired.com/politics/security/news/2007/08/epassport>

Hacked passport crashes readers

A hacker has demonstrated an exploit against the RFID tags in
the new US
passports that allows him to clone a passport and modify the
RFID with bad
code that will crash the passport readers. Lukas Grunwald, an
RFID expert
who has served as an e-passport consultant to the German
parliament, says
the security flaws allow someone to seize and clone the
fingerprint image
stored on the biometric e-passport, and to create a specially

coded chip
that attacks e-passport readers that attempt to scan it.

Grunwald says he's succeeded in sabotaging two passport readers made by different vendors by cloning a passport chip, then modifying the JPEG2000 image file containing the passport photo. Reading the modified image crashed the readers, which suggests they could be vulnerable to a code-injection exploit that might, for example, reprogram a reader to approve expired or forged passports.

"If you're able to crash something you are most likely able to exploit it," says Grunwald, who's scheduled to discuss the vulnerabilities this weekend at the annual DefCon hacker conference in Las Vegas.

✈ **IRS computer security/privacy problems**

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

Fri, 3 Aug 2007 10:47:55 PDT

The Treasury Inspector General for Tax Administration reports that in a recent test of 102 people with direct access to internal IRS data (employees and contractors), 62 of them complied with a request from a caller posing as a technical support person to provide their user name and temporarily change their password. Only eight called the IG's office or IRS security personnel to verify the identity of the caller. Similar tests in 2001 and 2004 were intended to improve security practices, but apparently were not effective.

investigating
to try to find out) what this imposed upgrade actually was.

Most significantly, if I had done nothing, my computer evidently would have rebooted, all by itself, in less than five minutes. But of course I had several windows open, containing all sorts of context relevant to the problem I was working on and which I most certainly did not want to log off and lose just then. And I was turning back and forth between the Windows computer and another one; I could easily have turned away for more than five minutes, and missed this charming little dialog box entirely.

Naturally I clicked "Restart later", and the dialog box went away. But about five minutes later it reappeared, exactly as before. I clicked "Restart later" again. About five minutes later it reappeared. I clicked "Restart later" again. This went on for the next hour or two.

In what universe is this acceptable behavior? I've got work to do; I don't have time for unprovoked restarts; I'd really rather not have to keep a weather eye on a machine so as to be able to repeatedly click "Restart later" just to keep the damn thing up and my work intact. I can't help but wonder what might happen with a machine being used for vital real-time work, or as an unattended server.

I do know the answer to the "In what universe?" question, of course: in Microsoft's universe. And I suspect that the update they were so insistent on applying was one for their benefit, not mine.

I further suspect I know (although it wouldn't say so) what the whether-I-liked-it-or-not upgrade specifically was. A couple of weeks ago the same machine had been asking me if I wanted to (voluntarily) install and activate another update, namely a more-fully-functional version of its "Windows Genuine Advantage" component. But I had declined that upgrade, because I know that the machine's software is genuine, and I don't want the machine "phoning home" all the time or complaining if it can't, and I certainly don't want it locking me out some day if it ever makes a mistake.

I hadn't noticed that it had stopped asking about that earlier upgrade. Perhaps I ought to have been suspicious. Like the back-alley con man who is perfectly happy to rob you if you decline the proffered game of three-card monte, I suspect Windows simply decided to fall back on "Plan B" after I declined the "voluntary" upgrade too many times. That machine is probably now assimilated, and I can feel secure that it is WGA-safe from non-genuine software. Yippee.

🚩 Location-Based Dictionary Attacks

<Diomidis Spinellis <dds@aueb.gr>>

Thu, 02 Aug 2007 10:08:29 +0300

I get daily security reports from the hosts I manage. Typically these contain invalid user attempts for users like guest, www, and root.

(Although FreeBSD doesn't allow remote logins for root, I was surprised to find out that many Linux distributions allow them.)

Today's log surprised me, because it contained only Greek names. Here is an excerpt from the log.

```
Aug  1 00:19:42 istlab sshd[22137]: Invalid user achaikos from
210.17.252.20
Aug  1 00:19:45 istlab sshd[22191]: Invalid user achilleus from
210.17.252.20
Aug  1 00:19:48 istlab sshd[22218]: Invalid user actaeon from
210.17.252.20
Aug  1 00:19:51 istlab sshd[22244]: Invalid user acteon from
210.17.252.20
Aug  1 00:19:55 istlab sshd[22279]: Invalid user adelpha from
210.17.252.20
Aug  1 00:19:58 istlab sshd[22302]: Invalid user adelphe from
210.17.252.20
Aug  1 00:20:01 istlab sshd[22321]: Invalid user adelphie from
210.17.252.20
Aug  1 00:20:04 istlab sshd[22353]: Invalid user adonia from
210.17.252.20
Aug  1 00:20:08 istlab sshd[22387]: Invalid user adonis from
210.17.252.20
Aug  1 00:20:11 istlab sshd[22400]: Invalid user adrasteia from
210.17.252.20
Aug  1 00:20:14 istlab sshd[22417]: Invalid user adrastus from
210.17.252.20
```

The attack to this host (which is based in Athens, Greece) came from a Hong-Kong-based machine, and the list contained many exotic Greek names while also missing many common ones. Therefore, I doubt that this was a local attack. A Google search revealed that the name list was obtained by merging male Greek names and female Greek names from <http://www.20000-names.com>. Most probably an attack tool contains lists of names for specific countries (the same site also provides,

African, Chinese, English, French, German, Hebrew, Irish, Italian, Japanese, Polish, Spanish, and Welsh names). The tool also maps the IP address of the host it attacks to a specific country, for instance, through the geolocation data of the IP-to-Country databases <http://ip-to-country.webhosting.info/>. Finally, the attack tool uses the country-specific list for trying to log in to those accounts. Attackers seem to be getting more sophisticated with every passing day.

Diomidis Spinellis - <http://www.dmst.aueb.gr/dds>

Amazon chasing 2-cent Web services bill

<"Martin Redington" <martin@mildmanneredindustries.com>>

Fri, 3 Aug 2007 02:19:36 +0100

I recently signed up for an Amazon Web services account, to try out their S3 service, supplying my credit card number for them to bill me. I played with the service very briefly, enough to incur \$0.02 of charges, which appeared in the statement they sent me on Wednesday.

Today I received a notification from Amazon that their attempt to charge my credit card had failed (presumably because the amount was too low), and asking if I could amend my account with valid payment method.

Hopefully sanity checking will prevail before they start seriously chasing

me for the money.

Windows Live Messenger blocking even more completely innocuous text

<Cody Boisclair <cody@zone38.net>>

Wed, 1 Aug 2007 16:42:25 -0400

In [RISKS-24.35](#), there was an entry I submitted detailing how Microsoft's Windows Live Messenger service silently filtered out any message containing ".scr" or ".pif", in a very ham-handed attempt to prevent links to trojans from coming through.

Even more recently, Microsoft has decided that any IM containing the substring ".info" should be silently discarded.

Yes, that's right. In an attempt to combat links to malicious executables hosted on a few random .info domains, they've blocked every reference to an entire top-level domain... and even *that*, as heinous as it may be, isn't the full extent of the block. Sharing a link to an article on www.infoworld.com via Messenger will be a futile effort indeed, for instance. And good luck trying to ask other .NET developers whether `MessageBoxIcon.Information` is the best icon for a given dialog.

The RISKS here are enough to leave one speechless-- in more ways than one!

Cody "codeman38" Boisclair cody@zone38.net <http://www.zone38.net/>

⚡ Re: Accuracy of Hawkeye at Wimbledon (PGN, [RISKS-24.76](#))

<Paul Wallich <pw@panix.com>>

Tue, 31 Jul 2007 20:26:37 -0400

Under the most obvious assumptions about the distribution of "in" vs "out" in disputed calls, that would mean the system was performing worse than chance on its four worst days. That's really not good at all. (There are other plausible distributions, of course. If players object to any call they think has a reasonable possibility of being reverse to their advantage, including some where their objective judgment agrees with the call, that would mean the system was performing seriously worse than chance. If players only object to calls that they think were utterly bogus, the system might well be doing better than chance on disputed calls. Of course, in that case, it might still be doing worse than chance on close shots in general.)

⚡ Fraudproof voting protocols from scientists

<"Warren Smith" <warren.wds@gmail.com>>

Thu, 2 Aug 2007 09:44:42 -0400

Simple New Voting Protocols provide Ballot Secrecy AND Fraud Resistance

Conventional wisdom says elections with "secret ballots" are protected against vote-buying and coercion, while elections publicizing the list of all voters with their votes are immune to fraud -- but you can't have it both ways. In a paper at EVT 07 (Boston, 6 August) mathematicians Ronald L. Rivest and Warren D. Smith refute that conventional wisdom, potentially enabling a new level of voting integrity.

"You can have your cake and eat it too with some very simple new voting protocols," said Professor Daniel Sleator of Carnegie-Mellon's computer science department. "These are explainable to children. It's surprising this wasn't thought of 50 years ago."

Previous attempts to create such protocols have "succeeded" in mathematical senses, but only by employing very complicated cryptographic algorithms, challenging even for math PhDs. Humans can't vote in those systems without computer aid, which means that each voter would have to own a small computer "helper" they trusted to be running correct, unhacked, voting software.

Rivest & Smith's new protocols, called "VAV," "Twin," and "ThreeBallot," don't require computers or cryptography, and need only low-tech mechanical voting devices. In each, voters get take-home "receipts" they can use later to check their vote was correctly counted -- or prove fraud -- but which nevertheless bear absolutely no relation to that voter's vote, hence aren't helpful for vote-selling.

How can that be? Your take-home receipt in Twin is a copy of a random
other person's vote. In VAV, each voter casts two votes and one matching
"antivote" and gets a copy of one of these three (she chooses which) as her
receipt. Either way, the receipt has no logical relation to that voter's
vote.

All three Rivest-Smith protocols allow "mixing in" old-style unsafe ballots
with the new safe ones. That not only permits happy coexistence with voters
who don't want to use the new system, but also "contagiously protects" even
the unsafe ballots against fraud. "I really love this 'easy upgrade'
feature," said Doug Jones, former chair of Iowa voting systems examiners and
computer science professor at University of Iowa.

The Rivest-Smith protocols work with a wide variety of vote-totaling
systems, not just the "plurality" system most familiar in the USA.

"Plurality is a very poor voting system," said Guy Ottewell, an astronomer
and author regarded as the inventor of Approval Voting in 1968. "We've
known better ones for 200 years." "In plurality voting, it's 'name one
candidate then shut up'," said Ottewell. "With Approval, you name _all_ the
candidates you 'approve.' It's actually simpler because there is no special
rule outlawing 'overvoting,' and it both delivers more information in each
vote and allows voters to approve their true favorite without being
strategically foolish, so it's also more honest information."

But why would voters want dishonestly to vote for someone other than their true favorite? "Two words," said Ottewell. "Ralph Nader." "With approval voting, Nader voters aren't a problem, they're beneficial."

But Ottewell and Smith now instead advocate "Range voting," essentially the system used in the Olympics: as their vote, voters score all the candidates they want to within some fixed score-range (say 0 to 9); highest average wins. (Range becomes the same as Approval if the range is 0 and 1.) "Honeybees have been using range voting for millions of years, and my computer simulations indicate it outperforms every other common vote-totaling proposal," said Smith. ###

MORE INFO:

Fuller Story (including how VAV & Twin actually work):

<http://RangeVoting.org/>

RivSmiPRshort.html

Rivest-Smith actual paper: <http://www.math.temple.edu/~wds/homepage/tb8.pdf>

also in html:

<http://rangevoting.org/RivSmiTB.html>

Addenda to the paper:
<http://rangevoting.org/RivSmiTBadd.html>

<http://rangevoting.org/RivSmiTBadd.html>

Follow-up stories:

<http://rangevoting.org/>

RivSmiPRfollow.html

EVT 07 Conference:

<http://www.usenix.org/events/evt07/cfp/>

Center for Range Voting:

<http://RangeVoting.org>

Dr. Warren D. Smith 631-675-6128 warren.wds AT gmail.com
(prefer email)

<http://www.math.temple.edu/~wds/homepage/works.html>

*Approval & Range voting (AV & RV):

Guy Ottewell +1297-442247 guy AT universalworkshop.com

<http://www.universalworkshop.com>

*(AV, RV, and also most other vote-totaling systems too)

Prof. Steven Brams, NYU politics dept. 212-998-8510 steven.brams AT nyu.edu

(co-author of book "Approval Voting") FAX: 212-995-4184

*Computer Science:

Prof. Daniel Sleator, CMU CS dept. Office ph 412-268-7563, fax: 412-268-5576,

home ph: 412-HACKERS

REVIEW: "Implementing ITIL", Randy A. Steinberg

<Rob Slade <rMslade@shaw.ca>>

Wed, 01 Aug 2007 08:29:51 -0800

BKIMITIL.RVW 20070228

"Implementing ITIL", Randy A. Steinberg, 2005, 141206618-2

%A Randy A. Steinberg RandyASteinberg@aol.com

%C Suite 6E, 2333 Government Street, Victoria, BC V8T 4P4

%D 2005

%G 141206618-2

%I Trafford Publishing

%O 888-232-4444 FAX 250-383-6804 sales@trafford.Com

%O <http://www.amazon.com/exec/obidos/ASIN/1412066182/>

[robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/1412066182/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/1412066182/](http://www.amazon.co.uk/exec/obidos/ASIN/1412066182/robsladesinte-21)

[robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/1412066182/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/1412066182/](http://www.amazon.ca/exec/obidos/ASIN/1412066182/robsladesin03-20)

[robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/1412066182/robsladesin03-20)

%O Audience i- Tech 1 Writing 1 (see revfaq.htm for explanation)

%P 489 p.

%T "Implementing ITIL"

Chapter one notes that there are problems in how information technology (IT) works in supporting the enterprise. Steinberg does mention that there should be better integration of the various parts and functions

of IT service, that IT service management (ITSM) should be performed better, and that the Information Technology Infrastructure Library (ITIL) is a framework for improving ITSM, but does not, at this point, define either ITIL (and never does explain ITSM). Nine general principles for success are listed in chapter two. The precepts are sound (such as targeting the "Pareto" processes that are going to give you the best results for least effort), but vague: there are almost no details on how to accomplish this wonderful state. Chapter three provides a generic and rather terse outline of a general project management cycle, under the heading of a process for implementing ITSM over a period of a year. Modification of the culture of a corporation is a massive and difficult task: the suggestions in chapter four have some interesting and useful detail in regard to communications, but disregard the challenges involved. A catalogue of roles for large teams and projects is given in chapter five: this is probably too large for most ITSM ventures.

Chapters six through eleven outline the general stages in a project cycle, albeit with idiosyncratic names for most phases (and missing a few steps, such as requirements definition, testing, post-implementation assessment, and maintenance). The material is reasonable, although quite terse and vague. A great deal of space is devoted to forms, checklists, and questionnaires. These would probably be quite useful as templates for those

involved in an ITSM improvement project, but would have to be refined for a specific situation. "Vision," in chapter six, is basically the project concept or initiation phase. "Assessment" is given a separate chapter (seven), but seems to be part of the concept definition. Planning is in eight, and implementation in nine. "Initial wins" are described, in chapter ten, as small, quick projects that provide some early "high" returns on the efforts. The text outlines a management cycle for small projects and so duplicates a good deal of material that was presented earlier. There is also a list of initial win projects, although the value of most is questionable and they would have to be carefully reviewed for a specific environment. "Control work," in chapter eleven, is partly implementation of small projects, partly overall project documentation and management, and lots of workflow model charts: the content is rather a mixed bag.

Chapter twelve finally gets around to some details of ITIL: the text does, rather briefly, present the topical areas (known, in ITIL parlance, as processes) of the management of incidents, problems, change, release (of software), configuration, service levels, availability, capacity, continuity, finance, the service desk, and security. A poorly explained and formatted two-dimensional chart of the information flow between processes makes up chapter thirteen. Various software utilities and their bare-bones functions are listed in fourteen, while fifteen mentions miscellaneous documents related to the ITIL processes. Chapter sixteen has a terse

catalogue of roles and job descriptions for the processes.

Guiding

principles are defined, in chapter seventeen, in a way that is very similar

to vision or mission statements, albeit with somewhat more detail.

(ITIL is a decent overview of the provision of IT services, but note

that it has gaps. For example, incident response is seen only in terms of customer service, without any relation to security.

Security

management has solid and important directives on management, a holistic approach, policies, and audit, but when it comes to the actual provision of controls, the advice is to have proper ones, without much detail on what those might be.)

The title of the work is somewhat misleading. The largest part of the book

has to do with generic project management. ITIL does get some presentation,

but not until the book is more than half over. In addition, the work is

poorly structured and written. The end of chapter sixteen, as one example,

talks about roles for "ICT," but ICT is not defined until the end of chapter

seventeen (and then only as "Infrastructure Control"). The material is not

complicated, but the writing is frequently unclear, and it is only the

simplicity of the basic concepts that prevents the reader from getting lost.

(Sometimes the writing is completely off the wall. "Fix just one IT service

problem per day and within 90 days you will have made 107 service improvements" is clearly self-contradictory.)

For those who have not done much in the way of project management, there are

some helpful guides that will get you going (although you will need to check

in other references such as Scott Berkun's "The Art of Project

Management "

[cf. BKARPRMA.RVW] or "Applied Software Project Management" by
Stellman and

Greene [cf. BKAPSWPM.RVW] in order to deal with the missing
bits). For

those not familiar with ITIL, chapter twelve is a reasonable
introduction.

For those working to improve ITSM within their enterprises you
will probably

need a bit more help than is provided herein.

copyright Robert M. Slade, 2007 BKIMITIL.RVW 20070228

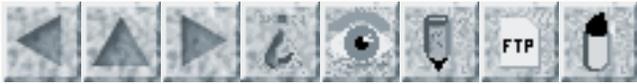
rslade@vcn.bc.ca slade@victoria.tc.ca

rslade@computercrime.org

<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

Search RISKS using [swish-e](#)

Volume 24: Issue 78

Wednesday 8 August 2007

Contents

- [San Francisco power outage](#)
[PGN](#)
- [US-VISIT problems](#)
[PGN](#)
- [PGN's Holistic Defective Agency](#)
[Peter Mellor](#)
- [Ounces, pounds, war, and the I-35W bridge](#)
[Sidney Markowitz](#)
- [Re: Comair Flight 5191](#)
[Erling Kristiansen](#)
- [A retrospective on an ARP spoofing attack...](#)
[Nicholas Weaver](#)
- [BotHunter: Detecting when a local system might be infected!](#)
[Phil Porras](#)
- [Legislation aims to end identity theft](#)
[Monty Solomon](#)
- [Bush Signs Law to Widen Legal Reach for Wiretapping](#)
[Monty Solomon](#)

- [Problem involving accidental misuse of someone else's credit card](#)
[Paul Robinson](#)
 - [Call For Search Engine Issues, Complaints, Concerns](#)
[Lauren Weinstein](#)
 - [Re: Accuracy of Hawkeye at Wimbledon](#)
[Mike Scott](#) [Michael Smith](#)
 - [REVIEW: "COSO Enterprise Risk Management", Robert R. Moeller](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ San Francisco power outage

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

Fri, 3 Aug 2007 15:29:31 PDT

At 1:49pm on 24 Jul 2007, 365 Main's San Francisco data center experienced a power surge when transformer breakers opened unexpectedly. Three of the ten backup generators failed to start, resulting in the loss of 40% of the customers. Attempts to close the breakers caused voltage fluctuations in PG&E's Martin Substation in Daly City. That resulted in a transformer failing in a manhole under 560 Mission Street. Between 30- and 50-thousand customers were out, in some cases up to two hours.

The final incident FAQ, with an introduction by Christopher M. Dolan, President and CEO, 365 Main Inc., is online, and worth reading.
http://www.365main.com/status_update.html

There is also an article in the San Francisco Chronicle that appeared online that evening. (Valleywag renamed the datacenter ``364.98 Main''.)

⚡ US-VISIT problems

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

Wed, 8 Aug 2007 6:30:49 PDT

US-VISIT (allocated \$1.7 billion since 2002), the U.S. government's main border control system, is plagued by computer security weaknesses, increasing the risk of computer attacks, data thefts, and manipulation of millions of identity records including passport, visa and Social Security numbers and the world's largest fingerprint database. A GAO report said "Weaknesses existed in all control areas and computing device types reviewed."

US-VISIT has compiled digital facial images and fingerprints of 90 million individuals and is used to vet 54 million border crossings each year. But Marc Rotenberg, executive director of the Electronic Privacy Information Center, said the government has not taken adequate steps to safeguard the privacy of millions of people whose citizenship, immigration, law enforcement and national security records are used in the customs checks.

[Border Computers Vulnerable to Attack GAO Report Details Problems in System, Spencer S. Hsu, *The Washington Post*, 3 Aug 2007; A02; PGN-ed]
<http://www.washingtonpost.com/wp-dyn/content/article/2007/08/02/AR2007080202260.html>

PGN's Holistic Defective Agency (Re: [RISKS-24.77](#))

<MellorPeter@aol.com>

Sun, 5 Aug 2007 14:31:43 EDT

So there was I thinking "Tsk. Can't even build bridges properly!"
and recalling Tacoma Narrows, the Hyatt Regency walkway, etc.

Then I recalled a few UK disasters:

Aberfan: Although the Coal Board (R.I.P.) had understood for years that spoil tips from coal mines could slip downwards and outwards catastrophically when wetted by rain, it took the deaths of around 70 Welsh schoolchildren to force action.

Ronan Point: No tie-bars in a tower block. A relatively small gas explosion in one flat blew out the walls and one whole corner of the block collapsed like a stack of cards.

Box Girder Bridges: Major problem for years with a cheap prefabricated method of constructing motorway bridges.

The "wobbly" Millennium Bridge: Well, I belong to a small but irritating minority that thinks it was more fun when it wobbled.

No doubt UK readers will be able to provide details of these and think of many more.

BTW (slightly related to PGN's mixed metaphor): Does anyone recall a demonstration by the Animal Liberation Front at which one of the

banners

read: "Free Schroedinger's Cat"?

BTW (even less related, but a variation on proverbs and metaphors): Dorothy

Parker, when asked to demonstrate the use of the word "horticulture", came up

with: "You can take a horticulture, but you can't make her think".

Peter Mellor; Mobile: 07914 045072; email: MellorPeter@aol.com

Telephone and Fax: +44 (0)20 8459 7669

★ Ounces, pounds, war, and the I-35W bridge

<Sidney Markowitz <sidney@sidney.com>>

Sat, 04 Aug 2007 17:08:49 +1200

I decided to look up some numbers to see how close the I-35W bridge disaster

is to the 1:16 ratio in the adage about ounces and pounds. For good measure,

I did some unit conversions to bring numbers in the millions and billions

down to small ones that people find easy to visualize.

This is all approximate to get the right order of magnitudes, based on new

reports that you can find through Google, so I'm not including links.

Congress allocated \$250 million to Minnesota for emergency repairs of the

bridge. Other news reports quote an estimate of what would be needed to

repair failing bridge infrastructure in the US of over \$9 billion per year

for 20 years, based on a figure of \$188 billion total required

to repair the estimated 73,533 "structurally deficient" bridges in the country. That comes out to an average of about \$2.5 million per bridge in repair costs. Currently only \$2 billion per year is being spent on such repairs.

On a separate topic, the Congressional Budget Office said that the Iraq war has cost about \$500 billion so far, or about \$10 billion/month or \$4000/second.

So it would have cost a little over 10 minutes of Iraq war expenditures to have repaired the I-35W bridge before it collapsed, and now it will cost about 100 bridges worth of preventative maintenance to repair this one bridge after the fact.

That doesn't add in the cost of loss of life, injuries and their aftermaths, destroyed cars, and the economic effect of the disruption to traffic with a major urban bridge down.

✶ Re: Comair Flight 5191 (Koenig, [RISKS-24.76](#))

<Erling Kristiansen <erling.kristiansen@xs4all.nl>>
Mon, 06 Aug 2007 18:04:04 +0200

Quoting from Department of Homeland Security, SECURITY IN THE SOFTWARE LIFECYCLE: Making Software Development Processes -- and Software Produced by Them -- More Secure, DRAFT Version 1.2 - August 2006, which in turn quotes from Dr. Nancy Leveson, A Systems-Theoretic Approach to

Safety in Software-Intensive Systems, *IEEE Transactions on Dependable and Secure Computing*, Vol. 1 No. 1, January-March 2004.

The assumption for almost all causal analysis for engineered systems today is a model of accidents (the safety corollary of security compromises) that assumes they result from a chain of failures and human errors. From an observed error, the analysis backward through the chain eventually stops at an event that is designated as the cause. A root cause selected from the chain of events usually has one or more of the following characteristics:

1. It represents a type of event that is familiar and thus easily acceptable as an explanation for the accident.
2. It is a deviation from a standard.
3. It is the first event in the backward chain for which a *cure* is known.
4. It is politically acceptable as the identified cause.

⚡ A retrospective on an ARP spoofing attack...

<Nicholas Weaver <nweaver@ICSI.Berkeley.EDU>>

Mon, 6 Aug 2007 09:33:04 -0700

<http://blogs.technet.com/neilcar/archive/2007/06/28/arp-cache-poisoning-incident.aspx>

Neil Carpenter, a Microsoft Escalation engineer on the PSS Security Support team, has a retrospective on his blog on an ARP-cache poisoning incident he was involved in analyzing.

In this case, the attacker used an arp-cache-poisoning transparent HTTP proxy to interrupt all HTTP requests and inject a piece of malicious attack code in a 0-size Iframe. Any vulnerable browser on the local network would quickly find itself infected with the malicious code.

The interesting thing was the automation: the automated tool, once installed on a victim, served to attack all the other systems. Also, the trick of looking at the MAC string to find the vendor tag seems a useful one to remember.

🔥 BotHunter: Detecting when a local system might be infected!

<Phil Porras <porras@csl.sri.com>>

Mon, 6 Aug 2007 12:40:38 PDT

One significant risk to those who spend lots of money on intrusion detection systems to monitor incoming network traffic is that they may grow to assume that outbound communications are not of high interest. In recent months a small group of researchers and I have been spending a significant amount of time developing a dialog-tracking engine to focus on the analysis of outbound traffic. In particular we've been interested in understanding the kinds of dialog interactions malware-infected local systems have with external systems.

Last week we made our dialog-correlation engine freely available

on the
Internet at <http://www.cyber-ta.org/BotHunter/>. BotHunter
should be of
interest particularly to security researchers and system
administrators.

To illustrate the effectiveness of BotHunter, the website
include a link to
our live malware analysis pages -- where we've been able to test
BotHunter
against roughly 9000 successful malware infections over the last
90 days.
The website includes the details of our system, including our
most recent
paper, which is being presented at this year's Usenix Security
Conference on
8 Aug 2007:

Guofei Gu, Phillip Porras, Vinod Yegneswaran, and Martin Fong,
BotHunter: Detecting Malware Infection through IDS-Driven
Dialog
Correlation

If you have doubts whether all the machines inside your network
perimeter
are infection-free, BotHunter may help you assess the "risks
from the
inside."

Phillip A. Porras (porras@csl.sri.com), Program Director, SRI
International
333 Ravenswood Ave, Menlo Park CA 94025 USA (650) 859-3232

[BotHunter seems to be attracting considerable interest. As
of this week,
it reached its first 1000 downloads. PGN]

Legislation aims to end identity theft

<Monty Solomon <monty@roscom.com>>

Sat, 4 Aug 2007 12:18:36 -0400

Dan Ring <dring@repub.com>, 4 Aug 2007

Massachusetts Governor Deval L. Patrick yesterday signed a bill designed to protect people against identity theft. The new law, which takes effect in 90 days, allows consumers to pay a \$5 fee to block access to their credit reports, forces companies and government agencies to notify people if personal information is lost or stolen and mandates disposal of certain personal information on consumers.

The law was approved following some highly-publicized thefts, including one reported in January by TJX Cos. in Framingham and another in May 2006 involving birth dates and Social Security numbers kept by the federal government of 26.5 million military veterans. ...

<http://www.masslive.com/hampfrank/republican/index.ssf?/base/news-10/1186212257204950.xml&coll=1>

An Act Relative To Security Freezes And Notification Of Data Breaches

<http://www.mass.gov/legis/laws/seslaw07/sl070082.htm>

An Act Relative to the Protection of Personal Information

<http://www.mass.gov/legis/bills/house/185/ht04pdf/ht04144.pdf>

Bush Signs Law to Widen Legal Reach for Wiretapping

<Monty Solomon <monty@roscom.com>>

Mon, 6 Aug 2007 08:42:28 -0400

President Bush signed into law on Sunday legislation that broadly expanded the government's authority to eavesdrop on the international telephone calls and e-mail messages of American citizens without warrants.

[Source: James Risen, *The New York Times*, 6 Aug 2007; PGN-ed]

Congressional aides and others familiar with the details of the law said that its impact went far beyond the small fixes that administration officials had said were needed to gather information about foreign terrorists. They said seemingly subtle changes in legislative language would sharply alter the legal limits on the government's ability to monitor millions of phone calls and e-mail messages going in and out of the United States.

They also said that the new law for the first time provided a legal framework for much of the surveillance without warrants that was being conducted in secret by the National Security Agency and outside the Foreign Intelligence Surveillance Act, the 1978 law that is supposed to regulate the way the government can listen to the private communications of American citizens. ...

<http://www.nytimes.com/2007/08/06/washington/06nsa.html?ex=1344052800&en=5e759f53fc811cd7&ei=5090>

⚡ Problem involving accidental misuse of someone else's credit card

<Paul Robinson <Paul@paul-robinson.us>>

Sat, 04 Aug 2007 05:51:24 -0400

I have had a problem involving use of someone else's credit card over the Internet. I want to post this because I want to advise people of a potential problem and/or risk and perhaps ask if someone else noticed this, or, in the alternative, make it known what happened so that people can be aware of it. Or maybe someone can tell me how this happened.

Another roommate who stays at the house I rent a room in uses my computer to handle his business, basically for surfing the net and such. If I'm at the computer I'm willing to help him find things or enter details. On occasion, typically for his customers he will book airline tickets, and he uses one specific credit card for that purpose. On occasion he's had me enter his information into the computer.

I do not know, and have never saved or captured his credit card information (I have my own cards). Well, what is weird is, there were two things I ordered which were charged to his card number. I haven't the slightest idea how. The last 4 digits of both cards are different, the issuers are not the same (the one I use belongs to a family member and is a major East-Coast bank, his has his name and is some small bank in the Midwest), and as I don't even know his number there's no way I could have used it intentionally.

My ATM card is on the Visa network, and if I hit a website that refused debit cards, I have a regular credit card which is issued to a

family

member, so I did not need to use someone else's card. And if I did need a credit card and did not have one around, I would have asked him first if I didn't have a credit card available.

I use Netscape version 7.2 "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.2) Gecko/20040804 Netscape/7.2 (ax)" on a Windows XP machine with Service Pack 2 for browsing because I do not trust Internet Explorer and its security holes. I have a hardware firewall between this computer and the Internet, so I can't argue some hacker broke in and switched one of my charges to his credit card. (Which is ridiculous to say the least.)

The only possible answer I can think of is that on one of the form fields used by one of the airline websites, is using the same field name as the two companies I ordered things from, and somehow they are capturing the same values from each other. (One was Vista Print, where I ordered two rubber stamps, and the other was AAA where I ordered a membership. I think the tickets he ordered were from Southwest Airlines.)

When I placed his legitimate order on Southwest, I typed in his number as he read it to me. I did not copy the number into the clipboard or otherwise save the number. Later when he saw his bill for two items he did not recognize and asked me about it, I discovered that the purchases he has on his bill exactly match the two I made, but should have gone on my credit card number. And I haven't the slightest idea how.

I went to Vistaprint's website, and tried a fake transaction. When I got to the payment page, where it asks for credit card number, the field is blank. I double-clicked on the credit card number field, and the previous value came up, with the correct card number (the one I would have used).

I don't know his number, didn't save it and did not attempt to use it. I couldn't have used his card number by mistake by typing in off of it if, I had, say, found it on the desk because he left it behind and I mistook it for one of the credit cards someone in my family has (first, the name would have been wrong and even if I didn't notice that, I would have spotted the credit cards as being wrong because I do not and have never used his bank.) But somehow I did use his card number and I haven't the slightest idea how. The only possible explanation I have is that some how form fields used on three different web sites are somehow cross-collecting information by pre-populating them, or something.

The two transactions together come to less than \$90, so it wasn't a huge issue, but it frightens me because I haven't the slightest idea how it happened or how I could have prevented it.

The solution I am going to use is that if I ever do anything for him that involves ordering something, I will use Internet Explorer (for accessing a specific known and trusted website, it is okay), and I will not use Netscape for anything he's using, as I only use Netscape for anything I

order. The only possible answer I can come up with is some form of cross-website contamination, which I do not believe could happen if I'm not using the same browser for any of his transactions, so I think this will solve the problem. I've also suggested he get his bank to issue him a new card with a different number.

This kind of thing scares me; if it wasn't for the fact he was understanding about it, I could technically have been looking at charges for credit card fraud! The thing that bothers me most is that I'll be damned if I can figure out how the hell this happened.

Call For Search Engine Issues, Complaints, Concerns

<Lauren Weinstein <lauren@vortex.com>>

Sun, 05 Aug 2007 22:32:19 -0700

Call For Search Engine Issues, Complaints, Concerns
<http://lauren.vortex.com/archive/000266.html>

Greetings. As part of my continuing research and an upcoming white paper focusing on policy and related technical issues associated with search engines and their impacts, I'd very much appreciate any examples of relevant specific situations, concerns, and any other positive or negative experiences with search engine operations and support personnel, with a particular emphasis on (but not limited to) the following categories:

- Attempts to remove or deemphasize from search engine listings
any data perceived to promote Web sites containing seriously
incorrect, defamatory, misleading, privacy-invasive, or otherwise highly damaging or problematic materials
- Search engine issues or problems related to "public record" (e.g. government) data, particularly with negative impacts on
privacy or individuals' personal lives
- Issues of "obsolete" or superseded data being promoted by search engine listings, without any indication that such data is no longer current and/or correct
- Any problems related to search engine caches exacerbating the sorts of issues listed above or other related problems
- And so on ...

I am particularly interested in any experiences you may have had while attempting to contact search engine personnel (either through provided Web forms or other means) with concerns or problems, and the dispositions of those communications.

For this round, I am specifically **not** soliciting issues related to "Search Engine Optimization" (SEO) concerns (e.g., "How come my Web site always ranks lower than that other Web site on Google?")

For any sagas you relate to me, please be as specific as possible (within whatever bounds that you feel comfortable) -- but at the very least please identify the particular search engine of concern and the approximate time period of the issue. Unless you specify otherwise, I will assume that I may note the issue (on an anonymous basis) in my reports on this subject. If you'd prefer that I don't

reference

your issue in any form, or if you don't mind being quoted non-anonymously for attribution, please let me know.

Please send any information that you can provide as soon as possible to:

search@pfir.org

For some recent background on the issues of concern, please see:

Search Engine Dispute Notifications: Request For Comments

<http://lauren.vortex.com/archive/000253.html>

Extending Google Blacklists for Dispute Resolutions

<http://lauren.vortex.com/archive/000254.html>

A Most Remarkable Google Page: Toward Search Dispute Resolutions

<http://lauren.vortex.com/archive/000255.html>

Benefits and Risks in Google's Public Records Access Project

<http://lauren.vortex.com/archive/000228.html>

Thanks very much!

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

+1 (818) 225-2800 <http://www.pfir.org/lauren> Blog: <http://lauren.vortex.com>

✶ Re: Accuracy of Hawkeye at Wimbledon ([RISKS-24.76](#))

<Mike Scott <usenet.11@data.scotts>>

Sat, 04 Aug 2007 11:04:12 +0100

The official Hawkeye website is a bit coy about details, but from <http://jtsang.blogspot.com/2006/07/technology-in-tennis-hawk-eye.html> it

looks as though 6 cameras are used - plus a /lot/ of processing

power and no
doubt many unpublished assumptions about ball dynamics (and some
errorless
code? :-)). It's a very high-tech solution, and vulnerable to
all sorts of
problems (calibration comes to mind; the claimed accuracy may be
quoted as
3mm - but one wonders what the error distribution looks like).

I've been racking my brains since my original submission to
RISKS, and still
can't see what would be wrong with a simple set of video cameras
(about 10
needed?) monitoring the various lines along with some simple
recording gear
with action replay, re-showing the real thing if needed. The
simulation is
very nice for TV to show details of players contact with the
ball - but why
is it necessary for line-call judgment? Technology for profit's
sake,
perhaps, plus the "king's new clothes" syndrome?

Mike Scott (unet <at> scottsonline.org.uk) Harlow Essex England

✶ Re: Accuracy of Hawkeye at Wimbledon ([RISKS-24.76](#))

<Michael Smith <emmenjay@zip.com.au>>

Mon, 06 Aug 2007 10:10:34 +1000

I suspect that we have misunderstood the process involved.

On serves, Hawkeye is used exclusively and to override it would
be quite
unusual. You do not generally see challenges on serves.

On other shots, by default, a human judge makes the call. If
the player

challenges that call, Hawkeye is used to adjudicate.

No information about the accuracy of Hawkeye can be determined from the situation. In fact, the process assumes Hawkeye is 100% accurate and makes no attempt to verify it. (Exactly how any verification might be conducted is not immediately obvious.)

⚡ **REVIEW: "COSO Enterprise Risk Management", Robert R. Moeller**

<Rob Slade <rMslade@shaw.ca>>

Mon, 06 Aug 2007 11:50:15 -0800

BKCOERM.RVW 20070506

"COSO Enterprise Risk Management", Robert R. Moeller, 2007,
0-471-74115-9

%A Robert R. Moeller

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 2007

%G 0-471-74115-9 978-0-471-74115-2

%I John Wiley & Sons, Inc.

%O 416-236-4433 fax: 416-236-4448

%O [http://www.amazon.com/exec/obidos/ASIN/0471741159/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0471741159/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/0471741159/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0471741159/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/0471741159/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0471741159/robsladesin03-20)

%O Audience i- Tech 1 Writing 1 (see revfaq.htm for explanation)

%P 367 p.

%T "COSO Enterprise Risk Management"

The inclusion of "COSO" (the Committee Of Sponsoring Organizations of

the Treadway Commission) in the title indicates that this work takes a corporate, and particularly financial, perspective with respect to risk management. The fact that the first paragraph of the preface makes reference to the key (if rather vague) phrase "internal controls" reinforces this idea. It is, therefore, somewhat ironic that the introduction complains that risk management is poorly defined and understood. The concept of internal control is similarly nebulous, and a badly understood abstraction can hardly be expected to result in advice likely to lead to solid implementations by the readers of the book.

Chapter one is a general introduction to the perceived need for COSO and internal controls. With yet more unintentional incongruity there is heavy emphasis on ethics and philosophy within the organization.

(An ethical enterprise would presumably have no need for internal controls.) A traditional risk management process is outlined in chapter two. (There is a great deal of consideration given to surveys, but little to either hard facts or statistics.) Chapter three's review of "enterprise" risk management reiterates a good deal of the previous material. The COSO risk management components are noted, mostly in regard to the highest corporate levels. The additional COSO dimensions of objectives and entity levels are covered in chapter four. Chapter five repeats content on roles, responsibilities, and process aspects of risk management. The history of the initial (1992 version) COSO structure is given in chapter six.

Chapter seven provides background on the Sarbanes-Oxley law, and some relations to the COSO framework. Audit is discussed in both

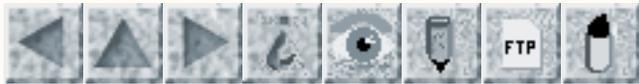
chapters

eight and nine, first with respect to the board, and then in regard to internal audit activities. The project management cycle is reviewed in chapter ten: unlike most similar pieces in risk management books, this one at least addresses specific functions regarding risk management. Chapter eleven purportedly ties enterprise risk management to information technology, but the topics are limited to application development, business continuity, and malware.

Chapter twelve's suggestions on building a risk culture follow the usual advice on creating a security awareness program. Various national financial standards and regulations are noted in chapter thirteen. In chapter fourteen the author ruminates on what should happen with risk management in the future.

This book is almost identical in content and style to numerous others on similar topics, such as Marchetti's "Beyond Sarbanes-Oxley Compliance" (cf. BKBYNSOX.RVW), "Security Controls for Sarbanes-Oxley Section 404 IT Compliance" by Brewer (cf. BKSCSOXC.RVW), Lahti and Peterson's "Sarbanes-Oxley IT Compliance Using COBIT and Open Source Tools" (cf. BKSIOITCU.RVW), and the rather better "Beyond COSO", by Steven J. Root (cf. BKBECOSO.RVW). The writing and material may provide some assistance with a risk management process, but the central points could have been provided in a clearer and more concise form.

copyright Robert M. Slade, 2007 BKCOSERM.RVW 20070506
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<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

Search RISKS using [swish-e](#)

Volume 24: Issue 79

Thursday 16 August 2007

Contents

- [Computer glitch holds up 20,000 at LAX](#)
[Paul Saffo](#)
- [LAX airport delay cause](#)
[David Magda](#)
- [U.S. legal time changing to UTC](#)
[Rob Seaman](#)
- [Source code at issue in drunk test](#)
[Ted Nelson](#)
- [Toll data nabs unfaithful spouses](#)
[Jonathan A. Marshall](#)
- [Voting excerpts from CRYPTO-GRAM](#)
[Bruce Schneier](#)
- [Computer-generated names](#)
[PGN](#)
- [Re: User-hostile behavior](#)
[Alexander Klimov](#)
- [Info on RISKS \(comp.risks\)](#)

Computer glitch holds up 20,000 at LAX

<Paul Saffo <paul@saffo.com>>

Sun, 12 Aug 2007 06:37:52 -0700

More than 20,000 international passengers were stranded for hours at Los Angeles International Airport on Saturday, 11 Aug 2007, waiting on airplanes and in packed customs halls while the malfunctioning of a computer system that determined who would be subject to secondary searches prevented officials from processing travelers entering the U.S. The system was down from 2pm until just after midnight, and the final passengers were not cleared until 3:50am -- except for six more requiring human intervention. As of 3am, some parking lots were still gridlocked.

"This is probably one of the worst days we've had. I've been with the agency for 30 years and I've never seen the system go down and stay down for as long as it did," said Peter Gordon, acting port director for customs.

[Source: Computer glitch holds up 20,000 at LAX; Passengers are delayed for hours on planes and in terminals after a customs processing system goes down. Karen Kaplan, Rong-Gong Lin II and Ari B. Bloomekatz, *Los Angeles Times*, 12 Aug 2007; PGN-ed]
<http://www.latimes.com/news/local/la-me-lax12aug12,0,5727961.story?coll=la-home-center>

✶ LAX airport delay cause

<dmagda@ee.ryerson.ca>

Wed, 15 Aug 2007 14:12:14 -0400 (EDT)

According to the *Los Angeles Times* (and an Associated Press article), the issue that caused thousands of travelers to be delayed at LAX was caused by a faulty network interface card (NIC) on a single machine:

> The card, which allows computers to connect to a local area network,
> experienced a partial failure that started about 12:50 p.m. Saturday,
> slowing down the system, said Jennifer Connors, a chief in the office of
> field operations for the Customs and Border Protection agency.
>
> As data overloaded the system, a domino effect occurred with other
> computer network cards, eventually causing a total system failure a
> little after 2 p.m., Connors said.

<http://www.latimes.com/news/nationworld/nation/la-me-lax15aug15,1,6802259.story?coll=la-headlines-nation>

<http://www.lompocrecord.com/articles/2007/08/15/ap-state-ca/d8r1dhl00.txt>

I've noticed on more than one occasion that often when the primary system breaks, and then fail-over occurs, the secondary system can't handle the backlog of requests.

When setting up new systems, two identically configured units are usually ordered and configured. Perhaps the secondary units should be more powerful as standard practice? Or the two should always run in parallel/

round-robin?

This way you know things are working on both, and if one goes away the second one is still around (in a known working state).

🚀 U.S. legal time changing to UTC

<Rob Seaman <seaman@noao.edu>>

Mon, 13 Aug 2007 02:06:52 -0700

H.R. 2272: the "21st Century Competitiveness Act of 2007" has been signed into law:

<http://www.govtrack.us/congress/bill.xpd?bill=h110-2272>

One of its provisions has changed the legal basis of U.S. timekeeping from mean solar time to UTC (Coordinated Universal Time). UTC (in its current form) has existed since the early 1970s, relying on the issuance of leap seconds every year or two to remain within 0.9 SI seconds of Greenwich Mean Time. Thus, if leap seconds continue, the effect of changing from mean solar time to UTC (overlaid by the standard time zones and varying Daylight Saving Time rules) is small for most purposes.

However, since 1999, ([feed://www.mail-archive.com/leapsecs@leapsecond.com](http://www.mail-archive.com/leapsecs@leapsecond.com)) the LEAPSECS forum has existed precisely to discuss the proposed elimination of leap seconds -- and thus the divergence of all civil and legal clocks from time as kept by the sun in the sky. With the passage of H. R. 2272, the

decision now rests not with the U.S. Congress, but with Working Party 7A of the Radiocommunication Sector of the International Telecommunication Union (ITU-R WP-7A):

<http://www.itu.int/pub/R-QUE-SG07.236>

Much of the LEAPSECS discussion has revolved around the large Y2K-like resource drain that the international astronomical community would face should UTC be redefined so as to no longer track mean solar time -- not only data structures would change, but also algorithms and runtime services. Now that UTC is legal time for the U.S., one wonders what similar expenses other sectors would face.

It is straightforward to show that civil timekeeping must track mean solar time closely:

- 1) Time kept by Mother Earth (mean solar time) differs from that kept by atomic clocks due to slowing caused by lunar tides. (There are many other periodic and aperiodic effects, but the tidal transfer of angular momentum accumulates secularly over long periods.)
- 2) Leap seconds are issued to compensate for the accumulation of a few milliseconds per day due to slowing that has already occurred, i.e., 2ms/day times 500 days would be one leap second even in the absence of further tidal effects. The solar day itself lengthens by just a few SI milliseconds per century.
- 3) With no leap seconds, day would literally turn into night

over a few

thousand years - i.e., this would be a redefinition of the much more fundamental concept of a "day".

4) There is a notion of embargoing leap seconds 3600 at a time into leap

hours as a kind of unfunded mandate placed on our N-great grandchildren.

Even those parties agitating for the cessation of leap seconds agree that

eventually they must still be released in such a larger jump.

5) A larger jump would be more disruptive than a smaller jump, therefore it

cannot be tolerated as frequently.

6) Pick a period of time over which a jump of such an amplitude would be

deemed too frequent. I suspect we could agree that one per century is

too many, but for the sake of argument let's specify the looser

constraint of a maximum of one leap hour per decade.

7) Simply divide. One hour per ten years = 3600 SI seconds per 3652 days.

QED. Civil time must track mean solar time to better than one SI second per

day. (In actuality, much better than one second.)

The fundamental challenge for precision timekeeping is that there are two

flavors of time: 1) the steady cadence of atomic clocks, and 2) the

wondering orientation of the Earth in space. A "second" is a unit with two

definitions that are often conflated. A second is either 1/86400 of a day,

or a second is the SI unit. In fact, the name first proposed for the SI

unit was the "essen", after Louis Essen, a pioneer timekeeper.

Much

confusion would have been saved if only this name had been chosen.

Q: What about apparent versus mean solar time?

A: A red herring. The Earth spins very regularly with respect to the stars.

Mean solar time is simply sidereal time offset by a little under four

minutes daily to account for the day "lost" each year from lapping the

Sun. That sundials run fast or slow at different times of year has

nothing to do with our clocks. People do care, however, whether the sun

is up at midnight in populated latitudes.

Q: Surely there have been professional meetings on this topic?

A: Yes, Torino in 2003. (http://www.gfy.ku.dk/~iag/ecag05doc/torino_coll.pdf)

The consensus was to leave UTC alone and that any civil timescale without

leap seconds should be called "TI" (International Time in the French

acronym). The ITU appears to have rejected this position.

Q: What's happened recently?

A: NASA has proposed a fall back recommendation making GPS time (with no

leap seconds) a standard interval time scale for precision timekeeping

projects, while leaving UTC alone:

<http://ussg7.org/documents/fact%20sheet%20modified%20and%20proposed%20new%20Recommendation.doc>

(This writer supports this recommendation.)

A couple of good references for leap second and general UTC information:

<http://www.ucolick.org/~sla/leapsecs>

<http://leapsecond.com>

My apologies for the length of this Risks submission. Confusion is often rife in even simple timekeeping applications.

Rob Seaman, National Optical Astronomy Observatory, Tucson, AZ

[Considering the plethora of calendar-clock-related cases reported in RISKS, this seems worthy despite its length. PGN]

🔥 Source code at issue in drunk test (via Dave Farber's IP)

<Ted Nelson <tandm@xanadu.net>>
August 12, 2007 4:16:34 PM EDT

This is like the voting-machine thing: citizen concern over what's inside the boxes we live with.

An attorney for a Minnesota man accused of drunken driving says he doesn't think the manufacturer of a breathalyzer will meet a court-imposed deadline of August 17 to turn over its source code.

If that happens, his client could go free.

As CNET News.com reported earlier this week, the Minnesota Supreme Court ruled late last month that source code for the Intoxilyzer 5000EN, made by a Kentucky-based company called CMI, must be handed to defense attorneys for use in a case involving charges of third-degree DUI against a man named Dale Lee Underdahl. CMI's historic resistance to such demands

has led to
charges being dropped in at least one case outside of
Minnesota. ...

http://news.zdnet.com/2100-1009_22-6202038.html

Theodor Holm Nelson, Founder, Project Xanadu; Visiting Fellow,
Oxford
Internet Institute; Visiting Professor, University of Southampton

IP Archives: <http://v2.listbox.com/member/archive/247/=now>

Toll data nabs unfaithful spouses

<"Jonathan A. Marshall" <marshall_mail@yahoo.com>>

Fri, 10 Aug 2007 15:59:18 -0400

Adulterers, beware: Your cheatin' heart might be exposed by E-ZPass.

Seven of the 12 E-ZPass states in the U.S. Northeast and Midwest provide

toll records to to court orders in criminal and civil cases.

Four of those

states (including NJ and PA) allow release only in criminal cases.

[Source: **Star-Ledger** by The Associated Press, 10 Aug 2007; PGN-ed]

<http://www.nj.com/news/index.ssf/2007/08/>

[toll_data_nabs_unfaithful_spou.html](http://www.nj.com/news/index.ssf/2007/08/toll_data_nabs_unfaithful_spou.html)

Voting excerpts from CRYPTO-GRAM

<Bruce Schneier <schneier@SCHNEIER.COM>>

Wed, 15 Aug 2007 03:34:56 -0500

[Note: This item has been PGN-excerpted with Bruce's permission. PGN]

CRYPTO-GRAM
August 15, 2007
by Bruce Schneier
Founder and CTO
BT Counterpane
schneier@schneier.com
<http://www.schneier.com>
<http://www.counterpane.com>

A free monthly newsletter providing summaries, analyses, insights, and commentaries on security: computer and otherwise. For back issues, or to subscribe, visit [<http://www.schneier.com/crypto-gram.html>](http://www.schneier.com/crypto-gram.html).

You can read this issue on the web at [<http://www.schneier.com/crypto-gram-0807.html>](http://www.schneier.com/crypto-gram-0807.html). These same essays appear in the "Schneier on Security" blog: [<http://www.schneier.com/blog>](http://www.schneier.com/blog). An RSS feed is available.

Assurance

Over the past several months, the state of California conducted the most comprehensive security review yet of electronic voting machines. People I consider to be security experts analyzed machines from three different manufacturers, performing both a red-team attack analysis and a detailed source code review. Serious flaws were discovered in all machines and, as a result, the machines were all decertified for use in California elections.

The reports are worth reading, as is much of the commentary on

the
topic. The reviewers were given an unrealistic timetable and had
trouble
getting needed documentation. The fact that major security
vulnerabilities were found in all machines is a testament to how
poorly
they were designed, not to the thoroughness of the analysis. Yet
California Secretary of State Debra Bowen has conditionally
recertified
the machines for use, as long as the makers fix the discovered
vulnerabilities and adhere to a lengthy list of security
requirements
designed to limit future security breaches and failures.

While this is a good effort, it has security completely
backward. It
begins with a presumption of security: If there are no known
vulnerabilities, the system must be secure. If there is a
vulnerability,
then once it's fixed, the system is again secure. How anyone
comes to
this presumption is a mystery to me. Is there any version of any
operating system anywhere where the last security bug was found
and
fixed? Is there a major piece of software anywhere that has
been, and
continues to be, vulnerability-free?

Yet again and again we react with surprise when a system has a
vulnerability. Last weekend at the hacker convention DefCon, I
saw new
attacks against supervisory control and data acquisition (SCADA)
systems
-- those are embedded control systems found in infrastructure
systems
like fuel pipelines and power transmission facilities --
electronic
badge-entry systems, MySpace, and the high-security locks used
in places
like the White House. I will guarantee you that the
manufacturers of
these systems all claimed they were secure, and that their
customers

believed them.

Earlier this month, the government disclosed that the computer system of the US-Visit border control system is full of security holes. Weaknesses existed in all control areas and computing device types reviewed, the report said. How exactly is this different from any large government database? I'm not surprised that the system is so insecure; I'm surprised that anyone is surprised.

We've been assured again and again that RFID passports are secure. When researcher Lukas Grunwald successfully cloned one last year at DefCon, industry experts told us there was little risk. This year, Grunwald revealed that he could use a cloned passport chip to sabotage passport readers. Government officials are again downplaying the significance of this result, although Grunwald speculates that this or another similar vulnerability could be used to take over passport readers and force them to accept fraudulent passports. Anyone care to guess who's more likely to be right?

It's all backward. Insecurity is the norm. If any system -- whether a voting machine, operating system, database, badge-entry system, RFID passport system, etc. -- is ever built completely vulnerability-free, it'll be the first time in the history of mankind. It's not a good bet.

Once you stop thinking about security backward, you immediately understand why the current software security paradigm of patching doesn't make us any more secure. If vulnerabilities are so

common,
finding a few doesn't materially reduce the quantity remaining.
A system
with 100 patched vulnerabilities isn't more secure than a system
with
10, nor is it less secure. A patched buffer overflow doesn't
mean that
there's one less way attackers can get into your system; it
means that
your design process was so lousy that it permitted buffer
overflows, and
there are probably thousands more lurking in your code.

Diebold Election Systems has patched a certain vulnerability in
its
voting-machine software twice, and each patch contained another
vulnerability. Don't tell me it's my job to find another
vulnerability
in the third patch; it's Diebold's job to convince me it has
finally
learned how to patch vulnerabilities properly.

Several years ago, former National Security Agency technical
director
Brian Snow began talking about the concept of "assurance" in
security.
Snow, who spent 35 years at the NSA building systems at security
levels
far higher than anything the commercial world deals with, told
audiences
that the agency couldn't use modern commercial systems with their
backward security thinking. Assurance was his antidote:

"Assurances are confidence-building activities demonstrating
that:

"1. The system's security policy is internally consistent and
reflects

the requirements of the organization,

"2. There are sufficient security functions to support the
security policy,

"3. The system functions to meet a desired set of properties and
only

those properties,

"4. The functions are implemented correctly, and
"5. The assurances *hold up* through the manufacturing, delivery and
life cycle of the system."

Basically, demonstrate that your system is secure, because I'm just not going to believe you otherwise.

Assurance is less about developing new security techniques than about using the ones we have. It's all the things described in books like "Building Secure Software," "Software Security," and "Writing Secure Code." It's some of what Microsoft is trying to do with its Security Development Lifecycle (SDL). It's the Department of Homeland Security's Build Security In program. It's what every aircraft manufacturer goes through before it puts a piece of software in a critical role on an aircraft. It's what the NSA demands before it purchases a piece of security equipment. As an industry, we know how to provide security assurance in software and systems; we just tend not to bother.

And most of the time, we don't care. Commercial software, as insecure as it is, is good enough for most purposes. And while backward security is more expensive over the life cycle of the software, it's cheaper where it counts: at the beginning. Most software companies are short-term smart to ignore the cost of never-ending patching, even though it's long-term dumb.

Assurance is expensive, in terms of money and time for both the process

and the documentation. But the NSA needs assurance for critical military systems; Boeing needs it for its avionics. And the government needs it more and more: for voting machines, for databases entrusted with our personal information, for electronic passports, for communications systems, for the computers and systems controlling our critical infrastructure. Assurance requirements should be common in IT contracts, not rare. It's time we stopped thinking backward and pretending that computers are secure until proven otherwise.

California reports:

http://www.sos.ca.gov/elections/elections_vsr.htm

Commentary and blog posts:

<http://www.freedom-to-tinker.com/?p=1181>

<http://blog.wired.com/27bstroke6/2007/07/ca-releases-res.html>

http://www.schneier.com/blog/archives/2007/07/california_voting.html

<http://www.freedom-to-tinker.com/?p=1184>

<http://blog.wired.com/27bstroke6/2007/08/ca-releases-sou.html>

<http://avi-rubin.blogspot.com/2007/08/california-source-code-study-results.html>

or <http://tinyurl.com/2bz7ks>

http://www.crypto.com/blog/ca_voting_report/

http://twistedphysics.typepad.com/cocktail_party_physics/2007/08/caveat-voter.html

or <http://tinyurl.com/2737c7>

http://www.schneier.com/blog/archives/2007/08/more_on_the_cal.html

California's recertification requirements:

<http://arstechnica.com/news.ars/post/20070806-california-to-recertify-insecure-voting-machines.html>

or <http://tinyurl.com/ytesbj>

DefCon reports:

<http://www.defcon.org/>

<http://www.physorg.com/news105533409.html>

<http://blog.wired.com/27bstroke6/2007/08/open-sesame-acc.html>

http://www.newsfactor.com/news/Social-Networking-Sites-Are-Vulnerable/story.xhtml?story_id=012000EW8420

or <http://tinyurl.com/22uoza>

<http://blog.wired.com/27bstroke6/2007/08/jennalynn-a-12-.html>

US-VISIT database vulnerabilities:

<http://www.washingtonpost.com/wp-dyn/content/article/2007/08/02/AR2007080202260.html>

or <http://tinyurl.com/33cglf>

RFID passport hacking:

<http://www.engadget.com/2006/08/03/german-hackers-clone-rfid-e-passports/>

or <http://tinyurl.com/sy439>

<http://www.rfidjournal.com/article/articleview/2559/2/1/>

<http://www.wired.com/politics/security/news/2007/08/epassport>

<http://money.cnn.com/2007/08/03/news/rfid/?postversion=2007080314>

How common are bugs:

<http://www.rtfm.com/bugrate.pdf>

Diebold patch:

http://www.schneier.com/blog/archives/2007/08/florida_evoting.html

Brian Snow on assurance:

<http://www.acsac.org/2005/papers/Snow.pdf>

Books on secure software development:

<http://www.amazon.com/Building-Secure-Software-Security-Problems/dp/020172152X/ref=counterpane/>

or <http://tinyurl.com/28p4hu>

<http://www.amazon.com/Software-Security-Building-Addison-Wesley/dp/0321356705/ref=counterpane/>

or <http://tinyurl.com/ypkkwk>

<http://www.amazon.com/Writing-Secure-Second-Michael-Howard/dp/0735617228/ref=counterpane/>

or <http://tinyurl.com/2f5mdt>

Microsoft's SDL:

<http://www.microsoft.com/MSPress/books/8753.asp>

DHS's Build Security In program:

<https://buildsecurityin.us-cert.gov/daisy/bsi/home.html>

This essay originally appeared on Wired.com.

[http://www.wired.com/politics/security/commentary/
securitymatters/2007/08/securitymatters_0809](http://www.wired.com/politics/security/commentary/securitymatters/2007/08/securitymatters_0809)

or <http://tinyurl.com/2nyo8c>

** ***

More Voting News

California Secretary of State Bowen's certification decisions are online. She has totally decertified the ES&S Inkavote Plus system, used in L.A. County, because of ES&S noncompliance with the Top to Bottom Review. The Diebold and Sequoia systems have been decertified and conditionally recertified. The same was done with one Hart Intercivic system (system 6.2.1). (Certification of the Hart system 6.1 was voluntarily withdrawn.) To those who thought she was staging this review as security theater, this seems like evidence to the contrary. She wants to do the right thing, but has no idea how to conduct a security review.

http://www.sos.ca.gov/elections/elections_vsr.htm

[http://www.nytimes.com/2007/08/05/us/05vote.html?
_r=1&adxnln=1&oref=slogin&adxnlnx=1186287020-kh0/
ehBMuFtZIyeXCC4wHg](http://www.nytimes.com/2007/08/05/us/05vote.html?_r=1&adxnln=1&oref=slogin&adxnlnx=1186287020-kh0/ehBMuFtZIyeXCC4wHg)

or <http://tinyurl.com/yto8ss>

Florida just recently released another study of the Diebold voting machines. They -- and it was real security researchers like the

California study, and not posers -- studied v4.6.5 of the Diebold TSx and v1.96.8 of the Diebold Optical Scan. (California studied older versions (v4.6.4 of the TSx and v1.96.6 of the Optical Scan).
<http://www.sait.fsu.edu/news/2007-07-31.shtml>
<http://election.dos.state.fl.us/pdf/SAITreport.pdf>

The most interesting issues are (1) Diebold's apparent "find-then-patch" approach to computer security, and (2) Diebold's lousy use of cryptography. More here:
http://www.schneier.com/blog/archives/2007/08/florida_evoing.html

The UK Electoral Commission released a report on the 2007 e-voting and e-counting pilots. The results are none too good.
<http://www.electoralcommission.org.uk/elections/pilotsmay2007.cfm>
<http://www.lightbluetouchpaper.org/2007/08/02/electoral-commission-releases-e-voting-and-e-counting-reports>
or <http://tinyurl.com/yukeot>

And the Brennan Center released a report on post-election audits:
http://www.brennancenter.org/dynamic/subpages/download_file_50089.pdf

My previous essays on electronic voting, from 2004:
<http://www.schneier.com/crypto-gram-0411.html#1>
<http://www.schneier.com/crypto-gram-0411.html#2>

My previous essay on electronic voting, from 2000:
<http://www.schneier.com/crypto-gram-0012.html#1>

** ***

CRYPTO-GRAM is written by Bruce Schneier. Schneier is the author of the best sellers "Beyond Fear," "Secrets and Lies," and "Applied Cryptography," and an inventor of the Blowfish and Twofish algorithms. He is founder and CTO of BT Counterpane, and is a member of the Board of Directors

of the
Electronic Privacy Information Center (EPIC). He is a frequent
writer and
lecturer on security topics. See <<http://www.schneier.com>>.

Crypto-Gram is a personal newsletter. Opinions expressed are not
necessarily those of BT or BT Counterpane.

Copyright (c) 2007 by Bruce Schneier.

✶ Computer-generated names

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

Tue, 14 Aug 2007 15:07:10 PDT

This is amusing, but not particularly unusual -- the computer
programmed
elision of an overly long concatenation of individual and
company names
where a new-line character presumably was omitted.

I just received an "Exclusive Platinum Visa Offer" from First
Equity in Fort
Mill, South Carolina, addressed to

Peter G. Nmnsri Intrntnl

offering a credit line up to \$100K, no annual fee, low rates,
and 5% cash
back. The form is of course already filled in with the above
name and
offers an immediate cash advance. I wonder whether a routine
credit check
would cause the application to bounce? Or perhaps they are so
eager for new
customers that they don't even bother with credit checks for
people
answering their preprinted exclusive-offer applications? Or

perhaps it is
a total scam? Well, a Web search gives me the assurance that

"During the last five years First Equity has not been
convicted in a
criminal proceeding, nor has it been a party to a civil
proceeding of a
judicial or administrative body of competent jurisdiction."

That is certainly reassuring, but makes one wonder about the
preceding
years. On the other hand, I certainly have enough credit cards
already.

✉ **Re: User-hostile behavior (Summit, [RISKS-24.77](#))**

<Alexander Klimov <alserkli@inbox.ru>>
Wed, 15 Aug 2007 16:16:08 +0300 (IDT)

I guess it is done this way on purpose: average user does not
understand why
they must patch the system and if there is an option on the
dialog 'I'll
reboot myself', most users will choose it without thinking.
There is a way
to stop this countdown: go to services (e.g., Win-R services.msc
Enter) and
stop 'Automatic Updates'), but this hidden option is akin to
self-moderation
of alt.sysadmin.recovery -- if one cannot find it, most likely
they do not
understand the security implications (of course, there is a risk
of
security-savvy users who are new to Windows).

Although, in my opinion, the solution is best for given problem
of forcing
reboot on novices, in a reasonable system there should be no

need to reboot
for update.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 80

Monday 20 August 2007

Contents

- [Vista prevents users from playing high-def content](#)
[Jon Brodtkin via Monty Solomon](#)
- [Software bug took Skype out](#)
[Wolfgang Bruener via Mark J Bennison](#)
- [Hacking The iPhone, Andy Greenberg on Black Hat](#)
[via Monty Solomon](#)
- [Google mistakes own blog for spam, deletes it](#)
[Robert McMillan via Monty Solomon](#)
- [Concern Over Wider Spying Under New Law](#)
[Risen-Lichtblau via Monty Solomon](#)
- [Risks of trusting your fonts?](#)
[Boyd Adamson](#)
- [Credit card headaches from TJX breach remain](#)
[Monty Solomon](#)
- [Cost of data breach at TJX soars to \\$256m](#)
[Monty Solomon](#)
- [Re: LAX airport delay cause](#)
[Olivier MJ Crepin-Leblond Hugu](#)

- [Re: Source code at issue in drunk test](#)
[Steven M. Bellovin](#)
 - [Re: Toll data nabs unfaithful spouses](#)
[David Lesher](#)
 - [Re: U.S. legal time changing to UTC](#)
[David E. Ross](#) [Randy Saunders](#) [Rob Seaman](#)
 - [Overreliance on voting technology?](#)
[Joseph Brennan](#)
 - [Everyone is getting on the "secure voting" bandwagon](#)
[Ferdinand J. Reinke](#)
 - [Search engines: too many users for personal assistance](#)
[Dan Jacobson](#)
 - [Save your transaction numbers!](#)
[Andrew Koenig](#)
 - [Wendy's: In the Clear](#)
[Gene Wirchenko](#)
 - [Re: ... misuse of someone else's credit card](#)
[Adrian Cherry](#)
 - [Engaging Privacy and Information Technology in a Digital Age](#)
[Jim Horning](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Vista prevents users from playing high-def content

<Monty Solomon <monty@roscom.com>>

Sat, 11 Aug 2007 12:02:16 -0400

Content protection features in Windows Vista are preventing customers from playing high-quality video and audio and harming system performance, even as Microsoft neglects security programs that could protect users, computer researcher Peter Gutmann argued at the USENIX Security Symposium in Boston [on 8 Aug 2007]. [Source: Content protection rules said to harm

system

performance, detract from security, Jon Brodtkin, NetworkWorld.com, 9 Aug 2007]

<http://www.networkworld.com/news/2007/080907-vista-high-def.html>

Software bug took Skype out

<"Bennison, Mark J" <mark.m.bennison@mbda.co.uk>>

Mon, 20 Aug 2007 08:06:20 +0100

[Source: Wolfgang Gruener, *TGDaily* 20 Aug 2007]

<http://www.tgdaily.com/content/view/33452/103/>

Skype today provided a few more information pieces about the reasons behind its massive network outage last week. According to the company, the network outage was initially caused by a "massive restart of [its] user's computers across the globe within a very short timeframe as they rebooted after receiving a routine software update." That high number of reboots was followed by an equally high number of log-in requests, which resulted in what Skype calls a "chain reaction."

On the Skype blog, a company representative wrote that this event revealed a "previously unseen software bug within the network resource allocation algorithm" which prevented Skype's "self-healing function from working quickly. ... Skype has now identified and already introduced a number of improvements to its software to ensure that our users will not

be similarly affected in the unlikely possibility of this combination of events recurring."

The company said that there were no malicious activities that impacted Skype.

[Also noted by Danny Burstein. PGN]

🔥 Hacking The iPhone, Andy Greenberg on Black Hat

<Monty Solomon [mailto:monty@roscom.com]>

Monday, August 06, 2007 1:44 PM

The Black Hat Conference
Hacking The iPhone
Andy Greenberg, 08.04.07, 2:02 PM ET

Don't say you weren't warned, iPhone fans. Even when the prerelease fervor surrounding Mac's mobile messiah-phone was at its highest, security researchers were warning that it would be vulnerable to exploitations like data theft and hijacking.

Last Thursday, Charlie Miller proved them right. In a presentation at the Black Hat conference in Las Vegas, a gathering of cyber-security researchers, Miller detailed how he had hacked and hijacked the iPhone by exploiting a vulnerability in its Web browser.

For iPhone owners, the talk wasn't as foreboding as it might have been. Apple had released a patch for Miller's exploit just days before. But Miller, a researcher at Independent Security Evaluators, says Apple's patch

was only possible because he had informed the company of the vulnerability weeks before he presented it to Black Hat's hacker audience. And, he says, it would only be a matter of time and effort to find an equally powerful backdoor into the phone.

Though there has yet to be any documented criminal hijacking of the iPhone outside of a lab, Miller says his research shows the relative ease of hacking smart phones, as well as Macs in general. He spoke with Forbes.com about the iPhone's vulnerabilities, Apple's short-lived patch and the company's undeserved reputation for building secure computers. ...

http://www.forbes.com/security/2007/08/04/iphone-apple-mac-tech-cx_ag_0804miller.html

Google mistakes own blog for spam, deletes it (Robert McMillan)

<Monty Solomon <monty@roscom.com>>
Sat, 11 Aug 2007 12:05:32 -0400

Robert McMillan, IDG News Service, 08/08/07

Readers of Google's Custom Search Blog were handed a bit of a surprise Tuesday when the Web site was temporarily removed from the blogosphere and hijacked by someone unaffiliated with the company.

The problem? Google had mistakenly identified its own blog as a spammer's site and handed it over to another person. ...

<http://www.networkworld.com/news/2007/080807-google-mistakes-own-blog-for.html>

⚡ Concern Over Wider Spying Under New Law

<Monty Solomon <monty@roscom.com>>

Sat, 18 Aug 2007 22:11:14 -0400

Broad new surveillance powers approved by Congress this month could allow the Bush administration to conduct spy operations that go well beyond wiretapping to include -- without court approval -- certain types of physical searches of American citizens and the collection of their business records. This offers a case study in how changing a few words in a complex piece of legislation has the potential to fundamentally alter the Foreign Intelligence Surveillance Act. [Source: James Risen and Eric Lichtblau, *The New York Times*, 19 Aug 2007; PGN-ed]
<http://www.nytimes.com/2007/08/19/washington/19fisa.html?ex=1345176000&en=2e7a7948ff52f9fe&ei=5090>

⚡ Risks of trusting your fonts?

<Boyd Adamson <boyd-adamson@usa.net>>

Mon, 20 Aug 2007 12:03:39 +1000

Jim Weirich, a prominent developer noticed that on his machine numbers were coming out incorrectly:

<http://onestepback.org/index.cgi/Tech/Mac/MyMacCantCount.red>

It seems that a corrupted "font cache" was causing all the "7" glyphs in a single font (in all apps) to display as "9".

Jim was doing web development. What would have happened if he were doing financial or life-critical systems work?

[It's a real glyph-hanger! PGN]

✂ Credit card headaches from TJX breach remain

<Monty Solomon <monty@roscom.com>>

Thu, 9 Aug 2007 09:01:04 -0400

Almost seven months after TJX Cos. revealed that at least 45.7 million credit and debit card numbers were compromised, some banks such as Citibank are still reissuing cards for customers whose information may have been exposed. ... [Source: Se Young Lee, *The Boston Globe*, 9 Aug 2007; PGN-ed]

http://www.boston.com/business/personalfinance/articles/2007/08/09/credit_card_headaches_from_tjx_breach_remain/

✂ Cost of data breach at TJX soars to \$256m

<Monty Solomon <monty@roscom.com>>

Fri, 17 Aug 2007 22:50:17 -0400

The figure is more than 10 times the roughly \$25 million TJX estimated just three months ago, though at the time it cautioned it didn't know the full extent of its exposure from the breach. The costs include fixing the company's computer system and dealing with lawsuits, investigations, and other claims stemming from the breach, which lasted more than a year before the company discovered the problem in December 2006. [Source: Ross Kerber, *The Boston Globe*, 15 Aug 2007; PGN-ed]
http://www.boston.com/business/globe/articles/2007/08/15/cost_of_data_breach_at_tjx_soars_to_256m/

✉ Re: LAX airport delay cause

<=?iso-8859-1?Q?Olivier_MJ_Cr=E9pin-Leblond?= <ocl@gih.com>>
Thu, 16 Aug 2007 21:58:57 +0200

This is a classic NIC fault. Without being in the know about LAX's specific failure, I suspect that all terminals are connected to large switches which simply act as relays to the backbone. On numerous occasions have I found NICs failing simply by either repeating any received packets, thus flooding the network, or worse still, not recognising potential collisions and therefore transmitting whilst other computers are transmitting at the same time. This results in a collision on each attempt. I've seen 100Mbit/s networks grind to a halt (0.1Mbit/s). As opposed to expensive backbone

telecom equipment, computer NICs are often cheap and nasty \$5 electronics.

The solution?

Don't put all your eggs in one basket.

Don't put all your computers on one sub-network.

Olivier Crepin-Leblond, PhD / Global Information Highway Ltd

⚡ Re: LAX airport delay cause (Magda, [RISKS-24.79](#))

<Huge <huge@huge.org.uk>>

Fri, 17 Aug 2007 15:07:07 +0100

What's happening at my place of employ is that the business are starting to query why we have duplicate systems "sat around doing nothing", so they start running production work on the DR kit. Then, when one site fails, the other can no longer cope with the workload.

⚡ Re: Source code at issue in drunk test ([RISKS 24.79](#))

<"Steven M. Bellovin" <smb@cs.columbia.edu>>

Thu, 16 Aug 2007 21:10:02 -0400

The Minnesota case relies on a rather narrow foundation: the RFP to which CMI responded gave title to at least some of the code to the state, and required CMI's co-operation with defense attorney requests. In other words, the Minnesota Supreme Court's ruling is not based on a recognition of a fundamental right as opposed to

the
factual basis of this particular case. I wonder, in fact, if
the prosecutors could secure a court order for the code under
contract
law, and enforce it with large civil damages.

More details on this in my blog entry on the case:

<http://www.cs.columbia.edu/~smb/blog/2007-08/2007-08-10.html>

✈ **Re: Toll data nabs unfaithful spouses ([RISKS-24.79](#))**

<"David Leshner" <wb8foz@panix.com>>

Thu, 16 Aug 2007 15:21:54 -0400 (EDT)

> Seven of the 12 E-ZPass states in the U.S. Northeast and
Midwest provide
> toll records to court orders in criminal and civil cases.
Four of those
> states (including NJ and PA) allow release only in criminal
cases.

A) Do they require a court order? [Or just a request?]

B) How do those states that do block civil demands accomplish
same?

[i.e. Do they have tested support in state law?]

C) What does this portend for other tracking records: NYC's new
access
charge scheme, DC Metro {and others, inc NYC..} permanent fare
cards, video
recordings, and cell phone tracking records? Does the alleged
protection
mentioned extend to them?

The obvious Risk: Mission Creep abounds. Will folks be required
to archive
all data just in case... How will the demand alter system

design? Staffing?

✉ Re: U.S. legal time changing to UTC

<"David E. Ross" <david@rossde.com>>

Thu, 16 Aug 2007 13:58:53 -0700

The elimination of leap-seconds is being promoted by those who are too lazy or too incompetent to code time conversions correctly. This situation arose because the long-term slowing of the earth's rotation (which creates the need for leap-seconds) failed to occur for several years, eliminating the need for leap-seconds for 7 years. Previously, a leap-second had been required every year or two.

From 1 January 1961 until 1 January 1972, UTC seconds varied in length relative to TAI seconds, leap-seconds were fractions of a second, and UTC clocks thus did not tick on the same instant as TAI clocks. I was a software test engineer on a project that handled this correctly.

UTC was redefined starting 1 January 1972 to have a second exactly the same as the TAI second, to have leap-seconds exactly whole seconds, and thus UTC clocks thereafter indeed did tick on the exact same instant as TAI clocks. The old software did not need revision; it still handled this correctly.

This was for a large software system for the command and control of military space satellites. Internal time was kept in TAI minutes from

some base time

because the mathematics required all minutes to be uniform in duration.

External time, however, was reported in UTC (day, month, year, hour, minute, and seconds -- to the nearest millisecond). UTC was also used as an

intermediate step to getting actual solar time (not mean solar time) for

determining the orientation of the surface of the earth relative to a fixed

coordinate system based on the stars.

When the software system was replaced in the mid-1980s, the developer (who

had not worked on the previous system) did not really understand the

difference between UTC and TAI. I repeatedly -- and unsuccessfully --

warned both the developer and the US Air Force (the customer) that there

would be problems for not doing time conversions correctly. In the end, the

Air Force was required to suspend mission operations a minute before a

leap-second and resume operations a minute after. This suspension was

considered to be a cost-effective response to the lack of proper design

because correcting the design would impact both software and hardware with a

cost of several millions of dollars (partially a consequence of poor

modularization of the software). A capability that existed in 1970 no

longer existed in 1992.

A historical tabulation of leap-seconds:

<http://hpiers.obspm.fr/eoppc/bul/bulc/UTC-TAI.history>

A history of the proposal to eliminate leap-seconds oriented against the

proposal:

<http://www.ucolick.org/~sla/leapsecs/nc1985wp7a.html>

David E. Ross <<http://www.rossde.com/>>

⚡ Re: U.S. legal time changing to UTC (Seaman, [RISKS-24.79](#))

<Randy Saunders <R.Saunders@ieee.org>>

Thu, 16 Aug 2007 15:26:57 -0400

We need to check our math here.

We're adding leap-seconds at a rate of less than one second per year. With 86400 seconds in a day, turning day to night takes more than 43,200 years. That's not a few to me, that's five times recorded human history.

Perhaps the time community will decide to add a leap-minute every 100 years or so. That's the sort of Y2K planning even Congress should be able to manage, and it only impacts folks who need to be within a minute of solar time. It would become the sort of once-in-a-lifetime event that century changes have been in the past. For a minute, about the time it took to read this "sky is falling" post.

Randy Saunders, JHU Applied Physics Lab +1.240.228.3861 R.
Saunders@IEEE.org

⚡ Re: U.S. legal time changing to UTC (Saunders, [RISKS-24.80](#))

<Rob Seaman <seaman@noao.edu>>

Thu, 16 Aug 2007 13:46:48 -0700

"Day into night" was poetic license to grab people's attention - apparently it worked.

Your calculation assumes a linear effect. The first leap hour is estimated to occur in about 600 years. They accelerate quadratically after that - remember, we have leap seconds due to the tidal slowing that has already occurred. Future slowing will make leap seconds occur more frequently. There have been the equivalent of about 4 leap hours since Aristotle's time:

<http://www.ucolick.org/~sla/leapsecs/ancient.png>

As I said, the expected cost to the astronomical community is large. One independent estimate was \$3M to remediate a single midsize telescope. The cost to other communities, as with Y2K, is unknown until an inventory is performed. This legislation guarantees, however, that researchers, government, and industry need to pay attention to UTC - now the law of the land. For instance, the impact of climate on our economy is ever more critically appreciated. Weather and tides, ocean currents and glaciers all respond to diurnal effects. The question isn't whether a static offset of a minute matters - the question is whether a residual secular slope of that magnitude matters. For many purposes, no. But is it prudent to assume that no risks possibly pertain?

We're all the "time community", of course.

Interested parties will find detailed, often entertaining, and sometimes repetitive discussion of these issues on the LEAPSECS mailing list:

<http://six.pairlist.net/mailman/listinfo/leapsecs>

Rob Seaman, National Optical Astronomy Observatory

⚡ Overreliance on voting technology?

<Joseph Brennan <brennan@columbia.edu>>

Thu, 16 Aug 2007 21:46:56 -0400

Imagine paper ballots, with a separate slip for each office that is up for election. Voters coming into the polling place would be handed a set of slips. They could be color coded, but also marked by number. The voters would first check that they have a complete set of slips.

The voters would then mark their choice of candidates on each slip, or write in any name wanted. They would put the slips into boxes for each color/number. (If a slip happens to go into the wrong box, that can be easily sorted out later by the poll counters.)

At the close of voting hours, poll counters would take each box in turn and sort the slips into piles for each candidate. In many cases the winner will be immediately apparent when one pile is obviously larger than the others. But of course exact counts would be made and reported. Poll watchers would watch the counting to be sure no one removes or adds slips.

After counting, the slips would be put into boxes and sealed.
If a recount
is called for later, the slips can simply be recounted.

Would an electronic system offer less opportunity for fraud, or
more
reliable detection of fraud? Would an electronic system be
cheaper to
implement? If no, why do we want electronic systems?

[This is of course a very old idea (used in many places more
or less as
proposed), but it keeps looking better and better when
observing the mad
feeding frenzy for all-electronic machines that have rushed in
where even
fools might fear to tread. PGN]

🔥 Everyone is getting on the "secure voting" bandwagon

<"r @ reinke" <reinke@reinke.cc>>

Thu, 16 Aug 2007 17:00:20 -0400

Go low tech on the counting side of the equation. By manually
counting
paper ballots, integrity and trust is restored. The time
savings and
convenience don't outweigh the costs when you factor in the
distrust a
closed, unverifiable system creates. For almost 200 years,
most elections
in the U.S. were handled this way. No, this doesn't alleviate
fraud. It
does potentially save billions of dollars to the taxpayer by
eliminating
unnecessary technology purchases while restoring
accountability in the
electoral system. Without accountability and transparency in
our electoral

system, technology additions do not provide any value no matter how persuasive are their advocates.

<http://www.lewrockwell.com/fisk/fisk9.html>

Even the political philosophy types understand that there's no confidence in any technology-based solution.

So why should us technology types keep pounding our collective heads against the walls?

Maybe the low tech solutions are really "the best" since they can be verified by the great unwashed and I include myself in that. Since the "kamikaze 1000", Dye boldly, or whatever isn't "my" platform of expertise, then I too am part of the great unwashed that doesn't understand it's particular version of "voo doo".

Some times one can be too smart for one's own good. There's no doubt that smart people can figure out a technological solution. And, there is equally also no doubt that the people, who seek to rule over others, are just as smart and cunning as well. Humans can always find a hole that they can exploit.

The old programming canard is so true, "you never find the last bug".

At least, the manual "one - two - three" doesn't require detailed examination. Just a counter and two or three watchers.

Ferdinand J. Reinke, Kendall Park, NJ 08824

<http://www.reinke.cc/> blog => <http://www.reinkefaceslife.com/>

⚡ Search engines: too many users for personal assistance

<jidanni@jidanni.org>

Mon, 13 Aug 2007 00:31:08 +0800

> attempting to contact search engine personnel

Why aren't search engine companies responsive to little old you and me?

Simple. Take why I dare not get hooked on their "gmail" product:

How can one

expect personal assistance when there are just too many users for the

company to provide personal assistance to?

⚡ Save your transaction numbers!

<"Andrew Koenig" <ark@acm.org>>

Sat, 11 Aug 2007 10:37:25 -0400

Between us, my wife and I have four credit cards, which you might think of

as "hers," "mine," "ours," and "business expenses." All four of those cards

are with Citibank, three in the guise of AT&T Universal Cards, and the

fourth directly.

The fourth card has significantly different properties from the other three,

despite being with the same bank. For one thing, it gives rebates on

various kinds of purchases, which can be spent (only) on buying or

maintaining an automobile. For another, the due date for

payments is a week before the statement date; on the other three cards, the two dates are the same.

Every month, a few days after statements become available, I go online and schedule electronic payments for all four cards. Although I am nervous about the possibility that a payment might wind up being credited for much more than I had requested, that is a possibility with paper checks also, and now that we don't get original checks back anyway, all such transactions come down to "he said, they said" anyway.

So...In the middle of last month, I scheduled payments for three credit cards (the fourth had a zero balance). A few days ago, I went back to check that the payments were in the queue as requested. To my surprise, (1) One of them had vanished, and (2) Even though the next statements had not yet been prepared, it was already past the due date.

I immediately scheduled another payment, which went through that day. Nevertheless, when the next statement came out, it included both a \$39 late fee and finance charges for all outstanding charges--even those that were to recent to appear on the statement.

I was able to get them to reverse those charges, based on their observation that I had paid the other cards at the same time. I still don't know what happened to this payment. Did I really forget one of the cards? Did I enter the transaction only to have it go awry somehow? I doubt I will ever

know.

But I do know that this would not have happened if, after seeing the final

confirmation screen, I had simply saved the date and confirmation number.

Yes, it is always possible for them to deny that the confirmation number

exists, just as it is possible to deny that a canceled check exists. But

it is much harder to do so, especially if they do not offer any alternative

means of proof.

Wendy's: In the Clear

<Gene Wirchenko <genew@ocis.net>>

Wed, 08 Aug 2007 16:10:09 -0700

Here is the text from a confirmation E-mail that I got from Wendy's Restaurant:

You are receiving this email because you (or someone pretending to be you)

has entered the WENDY'S KICK FOR A MILLION CONTEST. If you did not enter

this contest, please ignore this email.

This email confirms we have received your WENDY'S KICK FOR A MILLION

CONTEST entry information.

For your records, here is the password you used to register:
XXXXXXXXXX

[I changed the password in paragraph three. (sigh)]

Re: ... misuse of someone else's credit card (Robinson, [RISKS-24.78](#))

<"Adrian Cherry (UK)" <Adrian.Cherry@baesystems.com>>

Thu, 9 Aug 2007 13:56:34 +0100

> I use Netscape version 7.2 "Mozilla/5.0 (Windows; U; Windows NT 5.1;
> en-US; rv:1.7.2) Gecko/20040804 Netscape/7.2 (ax)" on a
> Windows XP machine
> with Service Pack 2 for browsing because I do not trust
> Internet Explorer
> and its security holes.

You could actually claim that Internet Explorer 7.x (IE7) is better than Netscape 7.x (N7) for security. Like anything with statistics it possible to interpret the numbers several ways. For checking browser security I would recommend <http://secunia.com/>

So N7 has 31 security issues against 15 with IE7. So N7 actually has more security holes than IE7 however on the bright side they are better at patching the security holes than Microsoft, N7 only has 4 outstanding security issues against IE7 with 9 still to fix, one of which is considered highly critical.

In fact if you want the most secure browsing then the latest version of Opera, www.opera.com is my recommendation, all 8 security issue have been patched by the vendor. From the website "There are no unpatched Secunia advisories affecting this product".

IE7 : <http://secunia.com/product/12366> Unpatched 60% (9 of 15
Secunia advisories)
N7 : <http://secunia.com/product/85> Unpatched 13% (4 of 31
Secunia advisories)
Opera 9 : <http://secunia.com/product/10615> Unpatched 0% (0 of 8
Secunia
advisories)

Engaging Privacy and Information Technology in a Digital Age

<"Horning, Jim" <Jim.Horning@sparta.com>>

Mon, 20 Aug 2007 12:57:13 -0700

(Re: Horning, [RISKS-24.68](#))

The abstract of the report titled in the above Subject line was included in

[RISKS-24.68](#), <http://catless.ncl.ac.uk/Risks/24.68.html#subj15>.

This report is now available from the National Academies Press, in hardcover or pdf download:

http://books.nap.edu/catalog.php?record_id=11896

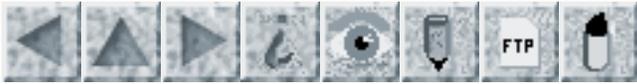
[This report was in the works for about five years. Jim's blog entry on it is online:

<http://horning.blogspot.com/2007/08/privacy-is-not-simple.html>

PGN]



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 81

Thursday 30 August 2007

Contents

- [Wells Fargo bank computer problem](#)
[Ted Lee](#)
- [MS WGA Servers down; XP & Vista installs marked "counterfeit"](#)
[David Lesher](#)
- [Tokyo subway train misses a station](#)
[Paul Saffo](#)
- [Free rides on the Boston T](#)
[Ryan Haggerty via Monty Solomon](#)
- [Skype outage resulted from flood of restarts after updates](#)
[PGN](#)
- [Problem that knocked out Skype has happened many times in the PSTN](#)
[Matt Holdrege](#)
- ["No trucks using satellite navigation"](#)
[Mark Brader](#)
- [Risks of randomly evaporating letters](#)
[Mark Brader](#)
- [Data thieves hit Monster.com site](#)
[Hiawatha Bray via Monty Solomon](#)

- [Even the Navy Can't Censor the Internet](#)
[Lauren Weinstein](#)
 - [Chinese Village Name Change Sparks Chaos](#)
[Mark Brader](#)
 - [With Software and Soldering, a Non-AT&T iPhone](#)
[Ken Knowlton](#)
 - [Cell phones swamping 911 systems](#)
[PGN](#)
 - [Cable Industry Responds Regarding HD TiVo Incompatibilities](#)
[Lauren Weinstein](#)
 - [E-voting predicament: Not-so-secret ballots, Declan McCullagh](#)
[PGN](#)
 - [The Risk Factor weblog](#)
[David Magda](#)
 - [Risks of a protocol mismatch](#)
[Dave Horsfall](#)
 - [More Wikipedia "Gotcha" Silliness](#)
[Lauren Weinstein](#)
 - [Suspect named in TJX credit card probe](#)
[Ross Kerber via Monty Solomon](#)
 - [Don't make the normal into the unusual - leap seconds vs hours](#)
[Guy Dawson](#)
 - [Amusing Lack of Software Support](#)
[Gene Wirchenko](#)
 - [Re: Risks of trusting your fonts?](#)
[McGrude](#)
 - [REVIEW: "Security Metrics", Andrew Jaquith](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Wells Fargo bank computer problem**

<"Ted Lee, Minnetonka, MN" <ted.lee@baesystems.com>>
Tue, 21 Aug 2007 14:07:18 -0500

I'm sure there will be several submissions on this. The associated press story on it contains the following "... Avid Modjtabai, head of technology for the nation's fifth largest bank, said today that problems with the company's online banking services lasted less than two hours, and customers never lost the ability to make basic ATM transactions, including withdrawing cash and making deposits at Wells Fargo-branded ATMs." While I haven't been able to verify that is the reason, on Sunday I had my Wells Fargo credit ("check") card refused by a merchant's POS terminal with the code "card blocked." My account has plenty of money in it and there are no untoward transactions in it. (That I was able to check. Go figure). I tried calling calling WF off and on all day yesterday to see if they knew why the card was blocked and they couldn't find out -- because their computers were down. Today I can't get through, presumably because of heavy call volume.

⚡ MS WGA Servers down; XP & Vista installs marked "counterfeit"

<"David Lesh" <wb8foz@panix.com>>
Sat, 25 Aug 2007 19:58:22 -0400 (EDT)

The Windows Genuine Disadvantage servers all went down.

Result: All attempted OS installations were labeled as counterfeit.

THAT means you get 'limp home' mode for the box..

<<http://forums.microsoft.com/Genuine/ShowPost.aspx?PostID=2053834&SiteID=25>>

<http://www.boingboing.net/2007/08/25/microsoft_wga_server.html>

The recovery procedure, once you know their server is again working, involves deleting some special files, and revisiting the WGA server.

{Sigh; haven't we had this conversation before?}

RISKS:

Creating an artificial single-point-of-failure.

Not making that single point robust/redundant enough to defend against all enemies, foreign and domestic [i.e. outsiders vs the more likely "we have met the enemy, and he is us..." errors.]

Not having good recovery procedure when the Can't Happen Does Happen... [Can your mother find her data.dat file?]

I wonder if the server farm has both geographic and network diversity.

(There was a Jan 2001 failure of all Microsoft nameservice; then, they were in one place, on one segment.)

I also worry about what happens if somehow, sometime, the MS database gets trashed, and it decides ALL copies of XP/VISTA/Win2009/whatever are pirated. So when every machine does its obligatory check-in, and gets castrated...

[Will Debian be VERY popular overnight?]

🔥 Tokyo subway train misses a station

<Paul Saffo <paul@saffo.com>>

Mon, 20 Aug 2007 21:53:36 -0700

[This looks like a RISKS story -- not to mention being a reminder of how quaintly peaceful a place Tokyo is that allows them to treat this as news.]

Subway train passes station after line switched to wrong track

A subway train was forced to pass a station it was supposed to stop at on Monday evening because the line was switched to a track exclusively for trains passing the station, the subway operator said.

At about 6:40 p.m., the driver of a local train on the Tokyo Metro Tozai Line slowed down his train to stop at Baraki-Nakayama Station in Funabashi, Chiba Prefecture, but noticed the train had gone onto the passing track, Tokyo Metro officials said.

The train was forced to continue on to the following Nishi-Funabashi Station. About 840 passengers were aboard the train but the incident did not cause major confusion.

Tokyo Metro officials pointed to the possibility that a computerized system controlling the line's railway switches had developed trouble. (Mainichi)

21 Aug 2007

<http://mdn.mainichi-msn.co.jp/national/news/20070821p2a00m0na003000c.html>

✶ Free rides on the Boston T

<Monty Solomon <monty@roscom.com>>

Thu, 23 Aug 2007 09:06:02 -0400

When the Boston Massachusetts Bay Transportation Authority updated its software to shut off about 13,000 lost, stolen, or expired cards, it also detected and disabled an unknown number of monthly passes that had been automatically reloaded without payment for up to the past seven months.

[Source: Ryan Haggerty, Glitch allowed free rides with T passes; Audit to check scope of flaw; firm blamed, *The Boston Globe*, 23 Aug 2007; PGN-ed]

http://www.boston.com/news/local/articles/2007/08/23/glitch_allowed_free_rides_with_t_passes/

✶ Skype outage resulted from flood of restarts after updates

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

Thu, 22 Aug 2007 18:42:09 PDT

For two days beginning on 16 Aug 2007, Skype's peer-to-peer network was critically unstable. This evidently resulted after Skype users all around the world rebooted their systems subsequent to getting a set of Microsoft patches via Windows Update. The flood of attempted Skype logins together with a lack of adequate Skype network resources at that time

prompted a chain reaction. Although this had never happened before, it revealed a flaw in Skype's self-healing mechanism -- which has now been fixed through retuning of the algorithms. This apparently had nothing to do with any particular MS patches. (Skype has something like 200 million users in total, although only 5 or 6 million are generally online at once. The peak usage reported was 9 million in January 2007.)

[Thanks to Lauren Weinstein for pointing out the Skype source with commentary by Villu Arak, 20 Aug 2007 and clarification on 21 Aug:

<http://heartbeat.skype.com>,

The site also includes current Skype status along with a note yesterday on a presumably temporary problem that involves payments using either of two banks in Estonia. PGN-ed]

⚡ Problem that knocked out Skype has happened many times in the PSTN

<Matt Holdrege <matt.holdrege@verizon.net>>

Tue, 21 Aug 2007 16:37:23 +0200

It is funny to see all the articles in Telecom magazines and blogs about how Skype is unreliable as proven by last week's outage. These people seem to forget that the vaunted PSTN has had many such outages. I posted here in RISKS back in 1993 about a Pacific Bell DACS software upgrade that went bad

and knocked out most of Orange County, California for a day. How often has the PSTN been killed by radio contests and natural disasters? Any large scale system can and will suffered from such problems as it is growing. This is nothing new to most RISKS readers.

✂ "No trucks using satellite navigation"

<msb@vex.net (Mark Brader)>

Tue, 28 Aug 2007 17:28:35 -0400 (EDT)

In the Welsh country borough known as Vale of Glamorgan, there have been several instances of foreign truck drivers following routings given by satellite navigation and apparently unable to understand signs reading "Unsuitable for heavy goods vehicles - Anaddas i gerbydau nwyddau trwm".

They are now experimenting with a pictographic sign instead -- showing a truck with a red slash through it, and a satellite overhead. To me this sign looks if heavy trucks whose drivers don't use satnav are now welcome...

<http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/08/28/nsatnav128.xml>
http://icwales.icnetwork.co.uk/0100news/0200wales/tm_headline=signs-to-warn-of-satnav-dangers&method=full&objectid=19695744&siteid=50082-name_page.html

Mark Brader, Toronto, msb@vex.net

⚡ Risks of randomly evaporating letters

<msb@vex.net (Mark Brader)>

Tue, 28 Aug 2007 23:46:22 -0400 (EDT)

The Saskatchewan Party is outraged that as the words Privatization of the Crowns fades out in one part of the ad, the letters P, O, R, and N stay up a split second longer than the rest.

http://www.ctv.ca/servlet/ArticleNews/print/CTVNews/20070828/sask_ad_070828/20070828/?hub=Politics&subhub=PrintStory

⚡ Data thieves hit Monster.com site (Hiawatha Bray)

<Monty Solomon <monty@roscom.com>>

Thu, 23 Aug 2007 08:52:21 -0400

Thousands of names, phone numbers, and e-mail addresses stored by the Internet job-search site Monster.com have been stolen as part of a complex online fraud scheme. Symantec Corp., a security company, disclosed the breach over the weekend after one of its researchers found that a server computer in Ukraine held 1.6 million records stolen from Monster, a New York company whose US operations are based in Maynard. [Source: Hiawatha Bray,

The Boston Globe, 22 Aug 2007: PGN-ed]

http://www.boston.com/business/globe/articles/2007/08/22/data_thieves_hit_monstercom_site/

✦ Even the Navy Can't Censor the Internet

<Lauren Weinstein <lauren@VORTEX.COM>>

Thu, 30 Aug 2007 07:48:44 -0700

<http://lauren.vortex.com/archive/000279.html>

I frequently make the assertion that it's impossible to successfully censor the Internet by trying to remove materials that have already been posted publicly after they've attracted attention. What's published is published, what's done is done. The genie won't just refuse to go back into the bottle, he'll stick his tongue out at you as well -- or worse.

You may recall the international brouhaha a couple of weeks ago over the Navy pulling from YouTube all copies of an (originally relatively obscure -- now infamous) amateur music video posted by a user named "PUMPIT01" and produced on the aircraft carrier Ronald Reagan (CVN76), as described in <http://tinyurl.com/2tuzdz> and many other stories.

The video in question ("Women of CVN76") has been variously described as being removed due to security violations (brief shots of utterly innocuous reactor-related areas), "inappropriate use of safety equipment," and other explanations.

The real reason for the Navy's "reaction" is clearly just plain old ordinary embarrassment, especially since the ship's CO has a cameo role

in the
amusing production.

But my point here isn't to post a video review, but rather to emphasize that for all the noise about deleting the video, it of course remains easily available with but a minimum amount of effort.

You may feel that the inability to effectively "recall" posted materials is a blow for freedom, or to the contrary an information control disaster. But either way, it's a fact -- a reality that we can't escape. And perhaps the sooner we come to terms with this truth, the less time we'll be wasting at shadow boxing with useless Internet censorship attempts. There are far better ways that we can be spending our time.

Excuse me? Oh, where's the video? Like I said, finding a copy is actually quite simple.

Example: For the sake of the argument, let's say that you did a Google Search right now for the straightforward query of:

cvn-76 women pumpit01 "click here"

No magic words. No secret codes. Just pretty obvious stuff from the news stories about the video, plus a little common search sense. And while any given search results are often fairly ephemeral, and any particular copy of material found at any given time may still be removed, well, the Internet is a big place, and the Lords of Censorship remain essentially impotent, for better or worse, indeed.

Lauren Weinstein +1 (818) 225-2800 <http://www.pfir.org/lauren>
lauren@vortex.com

⚡ Chinese Village Name Change Sparks Chaos

<msb@vex.net (Mark Brader)>

Tue, 21 Aug 2007 20:33:46 -0400 (EDT)

The 50 residents of the Chinese village Tianmeidong decided to change its name to one that would bring it better luck: Tianwei plus a third character that is rare enough that computers could not represent it. Even the Nanguo newspaper was forced to describe that character in its article because its computer could not write it. As a result, anything that involves the government is blocked, such as registering a marriage or the sale of property. [AP item, 21 Aug 2007, PGN-ed]

<http://www.guardian.co.uk/worldlatest/story/0,,-6865184,00.html>

Good luck with that character set!

⚡ With Software and Soldering, a Non-AT&T iPhone

<Ken Knowlton <KCKnowlton@aol.com>>

Sat, 25 Aug 2007 11:07:41 EDT

A 17-year-old New Jersey resident has published instructions on how to unlock Apple's iPhone so it will work on some competing cellular networks.

[Source: Brad Stone, *The New York Times*, 25 Aug 2007]
<http://www.nytimes.com/2007/08/25/technology/25iphone.html?th&emc=th>

🔥 Cell phones swamping 911 systems (*LATimes*)

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

Sun, 26 Aug 2007 9:33:09 PDT

An explosion in calls from cellular phones has overwhelmed critical parts of California's 911 system, resulting in hundreds of thousands of lost calls and lengthy waits to reach dispatchers even as crimes or potentially deadly emergencies unfold. Wireless 911 calls statewide have jumped roughly tenfold since 1990, to more than 8 million last year. Cell calls now make up the majority of all 911 calls, and key emergency agencies are struggling to adapt.

The problems are aggravated by call surges -- such as when multiple motorists call in about the same accident -- staffing shortages at 911 dispatch centers, and technological hurdles. Cell calls are more easily interrupted or lost and take longer to handle, officials say, reducing the number of calls each dispatcher can field.

[Source: Robert J. Lopez and Rich Connell, Users are experiencing lost calls and lengthy waits; Officials say it's better to summon help on a land line.

Los Angeles Times, 20 Aug 2007; PGN-ed]

<http://www.latimes.com/news/local/la-me-911cell26aug26,0,3741158.story?page=1&coll=la-home-center>

rich.connell@latimes.com and robert.lopez@latimes.com

🔥 Cable Industry Responds Regarding HD TiVo Incompatibilities

<Lauren Weinstein <lauren@vortex.com>>

Sat, 25 Aug 2007 14:05:04 -0700 (PDT)

Lauren Weinstein's Blog Update:

Cable Industry Responds Regarding HD TiVo Incompatibilities

August 25, 2007

<http://lauren.vortex.com/archive/000275.html>

[...] a few days ago I reviewed the situation concerning incompatibilities between the new High Definition TiVo ("TiVo HD") and the Switched Digital Video (SDV) systems being rapidly deployed by cable systems.

<http://lauren.vortex.com/archive/000273.html>

That was last Wednesday. The following day, that blog item appeared on Slashdot <http://www.slashdot.org> and was as a result very widely referenced and discussed. So much for Thursday.

Now comes word that the next day (yesterday), the cable industry trade association (NCTA - National Cable & Telecommunications Association)

<http://ibc.broadcastnewsroom.com/articles/viewarticle.jsp?id=175784>

made a filing with the FCC offering to develop a workaround for the problem.

As might be expected, NCTA is continuing to push the "OpenCable Application

Platform" (OCAP) system that the Consumer Electronics Association has found to be unacceptable.

However, NCTA reportedly says in their new FCC filing that they are now willing to develop a "tuning resolver" to work around the problem for existing devices like the new TiVo. This device would be a USB "dongle" to handle SDV tuning (the second of the probable options that I mentioned in my original blog item, as it happens).

While this is obviously a welcome development, two obvious questions are "When?" and "How much will it cost?"

Obviously cost is important. And if the device takes too long to appear, the associated host devices might already be obsolete!

Still, a busy three days, and no doubt the timing of the NCTA filing vs. all of the Slashdot attention to the issue was just an amusing coincidence.

⚡ E-voting predicament: Not-so-secret ballots, Declan McCullagh

<"Peter G. Neumann" <neumann@csl.sri.com>>
Mon, 20 Aug 2007 16:37:46 PDT

Ohio's method of conducting elections with ES&S electronic voting machines appears to have created a true privacy nightmare for state residents: revealing who voted for which candidates. Time-stamped paper trails permit the reconstruction of an election's results -- allowing voter

names to be

matched to their actual votes. [Source: Declan McCullagh, CNET News.com, 20

Aug 2007; PGN-ed from an interesting long article.]

http://news.com.com/E-voting+predicament+Not-so-secret+ballots/2100-1014_3-6203323.html

The Risk Factor weblog

<David Magda <dmagda@ee.ryerson.ca>>

Thu, 23 Aug 2007 10:46:21 -0400 (EDT)

The IEEE has a blog called "The Risk Factor" with the by-line "Software failures and successes dissected daily". Don't remember seeing it mentioned in RISKS, so I thought people might be interested:

<http://blogs.spectrum.ieee.org/riskfactor/>

Risks of a protocol mismatch

<Dave Horsfall <dave@horsfall.org>>

Wed, 22 Aug 2007 10:12:08 +1000 (EST)

When two similar protocols interoperate, the results can be drastic and at other times humorous; fortunately, this falls into the latter category:

<http://support.microsoft.com/kb/276304>

Looks like the response from the Kerberos server got mis-parsed by AD:

If you log on to an MIT realm, press CTRL+ALT+DELETE, click Change

Password, type your existing MIT password, and then type a new, simple

password that does not pass the dictionary check in Kadmind, you may

receive the following error message:

Your password must be at least 18770 characters and cannot repeat any of

your previous 30689 passwords. Please type a different password. Type a

password that meets these requirements in both text boxes. Note that

the number of required characters changes from 17,145 to 18,770 with the

installation of SP1.

NOTE: This is not a common case; it occurs only when you configure Windows

2000 to authenticate against an MIT Kerberos domain.

More Wikipedia "Gotcha" Silliness

<Lauren Weinstein <lauren@vortex.com>>

Sat, 18 Aug 2007 15:58:15 -0700 (PDT)

Lauren Weinstein's Blog Update: More Wikipedia "Gotcha" Silliness
August 18, 2007

<http://lauren.vortex.com/archive/000270.html>

My concerns regarding the Wikipedia operational model are fairly well known,

e.g., "Wikipedia and Responsibility"

<http://lauren.vortex.com/archive/000257.html>

So it was with considerable interest that I've noted the

controversy regarding a 24-year-old self-described "disruptive technologist," and his tool to more easily track the origin of Wikipedia changes (*The New York Times*, "Lifting Corporate Fingerprints From the Editing of Wikipedia").

<http://www.nytimes.com/2007/08/19/technology/19wikipedia.html>

But even the title of that article tends to belie the underlying nature of a real problem -- the lack of accountability for most of what's written or edited in Wikipedia. The "Corporate Fingerprints" bit is cute -- but what about all of the other fingerprints smeared through virtually every byte of the Wikipedia database?

Apparently it's one thing to snicker about corporate folks who want to correct what they perceive as errors (or, indeed, put their own positive spin on "the facts.") But there seems to be little interest in figuring out who purposely defaces pages, plants false or defaming information in the first place, or for that matter is responsible for the more mundane, probably factual minutiae, even just for the sake of establishing authenticity or expertise.

Wikipedia seems to be turning into a gigantic "gotcha" machine -- increasingly contaminated like a chunk of "Silly Putty" that's been used once too often to pick up comic strip images.

The single best thing that Wikipedia could do to lend itself genuine credibility would be to require that contributors identify themselves -- by name, not by handles or childish aliases. Or, as an alternative, at the

very least clearly indicate "in-line" when unauthenticated text dominates an entry.

Ironically, our disruptive technologist's tracing mechanism will probably have ever less value moving forward from today. While it will continue to be useful for retrospective analysis up to this point in time, we can be sure that more and more of the primarily targeted corporate Wikipedia editors will learn their lesson.

That lesson being, if you're going to edit your entry on Wikipedia, be sure to do it through a proxy or generic ISP account, not through your corporate network.

So moving forward, we'll probably have even less meaningful transparency concerning Wikipedia changes, and that Silly Putty Syndrome will likely continue to escalate.

Given what Wikipedia could aspire to be, that's really a shame.

✦ Suspect named in TJX credit card probe (Re: [RISKS-24.62,69,78,80](#))

<Monty Solomon <monty@roscom.com>>
Wed, 22 Aug 2007 01:21:54 -0400

[Source: Ross Kerber, *The Boston Globe*, 21 Aug 2007; PGN-ed]

Authorities have arrested Maksym Yastremskiy, a Ukrainian man, whom they

suspect played a key role in the sale of many credit card numbers stolen from TJX Cos., in what is considered the biggest corporate data breach to date. "Prices ranged from \$20 to \$100 per stolen card, and the cards were sold in batches of up to 10,000, depending on factors like the credit limits of the consumer accounts being traded."
http://www.boston.com/business/personalfinance/articles/2007/08/21/suspect_named_in_tjx_credit_card_probe/

⚡ Don't make the normal into the unusual - leap seconds vs hours

<Guy Dawson <guy@crossflight.co.uk>>

Tue, 21 Aug 2007 10:57:15 +0100

One of the risks of replacing frequent leap-seconds and thus the frequent need to handle them with infrequent leap-hours is that handling them becomes an unusual task.

We're never as good with unusual tasks as we are with the usual tasks.
Practice makes perfect!

With the requirement to add a leap second every few years systems have to be designed to handle them as part of their normal operation.

If we have to add a leap hour every 100 years or so, we'll have Y2K date problems every time. The same old excuses will be rolled out :

We never expected this system to have to handle leap hours when we built it.

Since leap seconds come around every few years any system that is to keep accurate time has to deal with them head on as part of the basic design.

Guy Dawson, I.T. Manager, Crossflight Ltd guy@crossflight.co.uk

⚡ Amusing Lack of Software Support

<Gene Wirchenko <genew@ocis.net>>

Sat, 25 Aug 2007 09:33:23 -0700

This story is hilarious:

The opening paragraph: "A Linux user who was jailed for uploading a film onto a peer-to-peer service has been told he will have to switch to Windows if he wants to use a computer again."

It seems that the monitoring software he is now required to have does not run under Linux. Also amusing is the closing remark about being *given* two felonies.

http://news.com.com/Linux+felon+forced+to+install+Windows/2100-1030_3-6204348.html?tag=nefd.pulse

⚡ Re: Risks of trusting your fonts? (Adamson, [RISKS-24.80](#))

<McGrude <mcgrude@gmail.com>>

Mon, 20 Aug 2007 17:56:51 -0700

But wasn't the only issue the *display* of the underlying data?

From the linked post, "copying and pasting what looks to be '0123456989' into a text editor will still give '0123456789'". [Typo in original linked post corrected. PGN]

From that I'd assume that internal calculations would still be correct and that only the displaying of results would be corrupt. It is still a problem, no doubt, but at least it wasn't as bad as it could have been.

Mike Hogsett

🔥 REVIEW: "Security Metrics", Andrew Jaquith

<Rob Slade <rMslade@shaw.ca>>

Wed, 29 Aug 2007 10:53:24 -0800

BKSECMTR.RVW 20070612

"Security Metrics", Andrew Jaquith, 2007, 0-321-34998-9,
U\$49.99/C\$61.99

%A Andrew Jaquith

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8

%D 2007

%G 0-321-34998-9 978-0-321-34998-9

%I Addison-Wesley Publishing Co.

%O U\$49.99/C\$61.99 fax: 416-443-0948 800-822-6339 bkexpress@aw.
com

%O [http://www.amazon.com/exec/obidos/ASIN/0321349989/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0321349989/robsladesinterne)

<http://www.amazon.co.uk/exec/obidos/ASIN/0321349989/>

[robsladesinte-21](#)

%O <http://www.amazon.ca/exec/obidos/ASIN/0321349989/>

[robsladesin03-20](#)

%O Audience i- Tech 1 Writing 1 (see revfaq.htm for explanation)

%P 306 p.

%T "Security Metrics: Replacing Fear, Uncertainty, and Doubt"

In the Foreword, Dan Geer states that the book is not about selling the idea of metrics. Which makes the initial chapters a bit problematic: if they aren't about selling the idea of metrics, what are they about? Chapter one is supposed to be an introduction, but seems primarily focused on the idea that metrics are not about risk management. (There is also an assertion that proper metrics are "well understood across industries, and consistently measured," which is interesting because much of what follows appears to contradict this statement.) The definition of security metrics, in chapter two, addresses metrics from fields other than security, and emphasizes the position that metrics are important (and that the current "metrics," such as checklist frameworks and annualized loss expectancy, are inadequate). Chapter three divides metrics into four general areas, dealing with perimeter security, control, availability, and applications development. Brief examples of collections of metrics related to these fields are given in the text, although the lists can't be expected to be comprehensive, due to the huge scope of security as a whole. The second of these topics, control, is probably the subject of chapter four, although it is entitled "Measuring Program Effectiveness." Basic concepts from

statistics, such as the difference between mean (average) and median (midpoint of a set of elements), are presented in chapter five. Chapter six talks about demonstrating data in a visual manner. Most of the material consists of suggestions for graphics and examples are given "redrawing" the displays of commercial programs. Aspects of automating the calculations of security metrics are outlined in chapter seven. In chapter eight, Jaquith recommends the use of a security scorecard based on the Balanced Scorecard management assessment model.

Security can be difficult to define, let alone measure, and, in general, too little attention is paid to numeric assessments that can assist in determining how well we are performing at the task. This book does go somewhat beyond a mere exhortation to create and use metrics for security, but it still leaves an awful lot of work for the practitioner or manager.

copyright Robert M. Slade, 2007 BKSECMTR.RVW 20070612
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>

[The need for incisive security metrics has been with us for a long time.

On the other hand, the metrics that have emerged tend to be local rather

than system-wide, and these local metrics are not easily composed into

system-wide metrics. Even the metrics for algorithmic crypto strength are

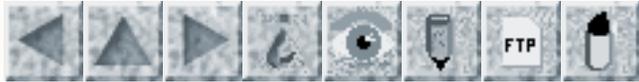
relatively unsatisfying when the crypto is poorly implemented or embedded

in systems that are easily compromised -- whether by insiders or outsiders.

Thus, the quest for meaningful system-level security metrics that can be

derived from lower-layer metrics remains an enormously difficult

challenge. 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

Search RISKS using [swish-e](#)

Volume 24: Issue 82

Wednesday 12 September 2007

Contents

- [Amtrak ticketing system outage](#)
[Steven M. Bellovin](#)
- [New Zealand: Telecom's NGN will make old phones obsolete](#)
[Henry Baker](#)
- [German rubbish piles up due to due to toll-system problems](#)
[Peter B. Ladkin](#)
- [Aircraft safety and software reliability](#)
[Phil Colbourn](#)
- [Risks of a flying society](#)
[Nick Brown](#)
- [Groklaw reports 'The Incredible "Lawyers as Hackers" Case'](#)
[Kelly Bert Manning](#)
- [EZ-pass evidence and the law](#)
[PGN](#)
- [On-line property assessment databases a bit too accessible](#)
[Jonathan Kamens](#)
- [Police mail sensitive information to the press](#)
[Debora Weber-Wulff](#)

- [iTunes sharing](#)
[Henry Baker](#)
 - [Security: an example from Pakistan](#)
[Dan Jacobson](#)
 - [Monster data capture also includes "USAJobs"](#)
[Jeremy Epstein](#)
 - [Redacted account numbers](#)
[Tom Watson](#)
 - [Re: Save your transaction numbers!](#)
[Diomidis Spinellis](#)
 - [Re: Chinese Village Name Change Sparks Chaos](#)
[Julian Bradfield](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Amtrak ticketing system outage

<"Steven M. Bellovin" <smb@cs.columbia.edu>>

Thu, 30 Aug 2007 16:03:25 -0400

On Saturday morning, 25 Aug 2007, the nationwide Amtrak ticketing system failed. It wasn't restored to service until early Sunday afternoon. During that time, passengers couldn't buy tickets except (sometimes) at a ticket window, query or change reservations, or retrieve previously-purchased tickets. Some other web functions were also unavailable.

The cause of the problem is unclear. More precisely, there have been two different, contradictory, explanations in the press. One version has it that they upgraded their software; the new version didn't work, and it took a long time to diagnose the problem and back out the changes. The other

story is that a circuit breaker panel failed, and it took a day to obtain a replacement.

There were good and bad aspects to how Amtrak handled. The most glaring failure was one of communications. Apart from the different stories about the cause, there was *no* mention on their web site about the problem. If you tried to buy tickets, you just received a "come back later" message.

The bright side is that Amtrak did have a contingency plan for this situation, even though it had never happened before. Passengers with reservations were supposed to board the train the conductor came around collecting reservation numbers. (It remains to be seen if I will encounter any residual billing or accounting difficulties from this happening to me. ... When I got to the station for my return trip, the automated kiosks were unable to handle the situation (and gave a poor error messages); the clerk, though, had no trouble when I explained the situation.) On the other hand, because this was such a rare situation, passengers at some stations were told they had to purchase new, hand-written tickets. Presumably, they'll receive refunds.

More details and press links in my blog entries:

<http://www.cs.columbia.edu/~smb/blog/2007-08/2007-08-26.html>

<http://www.cs.columbia.edu/~smb/blog/2007-08/2007-08-28.html>

Steve Bellovin, <http://www.cs.columbia.edu/~smb>

✦ New Zealand: Telecom's NGN will make old phones obsolete

<Henry Baker <hbaker1@pipeline.com>>

Fri, 07 Sep 2007 10:54:28 -0700

FYI -- You've heard of the demise of analogue TV's; now New Zealand is getting rid of analogue telephones. Aside from the issues of emergency access when electrical power is down, note the fact that the old dial-up "analog" modems will no longer work. While no one uses them much these days due to low bandwidth, they often provide the cheapest bit transmission around for email, and may be the last refuge of bit transmission still "net neutral".

Hundreds of thousands of conventional telephones that do not require mains

power and are instead powered off the phone network will not work once

Telecom switches to its Next-Generation Network, Telecom has confirmed.

Dial-up Internet access will also be withdrawn and analogue modems in

personal computers may not work, Telecom says. The switch-over from the

Public Switched Telephone Network (PSTN) to the NGN has been planned for

several years and is scheduled to be finished by 2012, though there is

growing speculation the completion date will be pushed back to 2015. From

then, customers will require a "residential gateway" device in their home

that will need mains power. ... [<http://www.stuff.co.nz/4178345a28.html>]

[Backup? We don't need no steenking backup when power is out -- especially in areas where cell phones don't work. PGN]

German rubbish piles up due to due to toll-system problems

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>
Mon, 10 Sep 2007 16:25:21 +0200

After a shaky and expensive start, it seems as if the automatic toll-collection system for trucks on the German Autobahn (freeway or turnpike, depending on if you are a car or a truck) is more or less working.

Unless you happen to be the Ferdinand Münnich Waste Disposal company in Lippstadt. Our local newspaper, the Neue Westfälische Zeitung, reported on the 10 July 2007 that their truck fleet was immobilised, pretty much from one second to the next, as the newspaper put it, at about 10 am on 19 March.

At that point, the company received phone calls from six of its drivers who were somewhere in Germany on the Autobahn. Their on-board toll machines were turned off, because the company's credit limit was exceeded. The company performs its toll transactions using the "Log-Pay-System", as do many companies which are continuously underway. This system extends credit for tolls automatically through a bank called the DVD-Bank until specific payment dates. DVD-Bank works with a collection agency, Creditreform, to protect itself from insolvent companies.

Apparently at Creditreform there was suddenly an "arrears advisory" concerning the firm. That was automatically forwarded to DVB-Bank, which shut off credit immediately and that in turn led Toll Collect to shut off the on-board systems so that the trucks could not roll further. It took a day to clear up the problem; meanwhile the truckers had to wait in Autobahn rest areas.

Apparently it was a mistake. However, Creditreform apparently doesn't (want to) take responsibility for the information it distributes. The bank is apparently saying that credit is a privilege, not a right, and trust in the customer (Münnich) was temporarily lost through the information from Creditreform until the problem was sorted out.

The company Münnich is trying to recover costs. As the paper put it in its subtitle "the involved (organisations) are washing their hands in their innocence".

Peter B. Ladkin Causalis Limited and the University of Bielefeld
www.causalis.com www.rvs.uni-bielefeld.de

✈ Aircraft safety and software reliability

<"phil colbourn" <philcolbourn@gmail.com>>

Sat, 1 Sep 2007 13:33:29 +1000

I have been reading "**Worst Case Reliability Prediction Based on*

a Prior

Estimate of Residual Defects" by *P.G. Bishop and R.E.

Bloomfield from the

*Thirteenth International Symposium on Software Reliability

Engineering

(ISSRE '02)*, November 12-15, Annapolis, Maryland, USA, 2002(c)

IEEE

http://www.adelard.com/papers/issre02_34_bishop.pdf

This paper and earlier work suggest that a software system failure rate can

be bounded by N/et where N is the number of (residual) faults at $T=0$, e is e

and t is the total usage time. The theory predicts (If I read it correctly)

reliability growth where a system can be assumed to have a finite number of

faults each with a constant failure rate.

I then happened upon this report from Boeing regarding air craft accidents.

<http://www.boeing.com/news/techissues/pdf/statsum.pdf>

It contains a graph of accidents from 1959 to 2006. The graph looked similar

to what would be predicted from a software system according to the theory.

I wonder... The aircraft industry (any industry that is focused on safety)

produces complex, multi-functional systems. The industry is based on

standards, engineering methods, maintenance procedures, failure investigation and corrective action. This seems very like the software

industry: requirements, coding standards, fault analysis and rectification.

Software is, after all, a set of procedures - ordered instructions to

perform some function.

Could it be that industry failure rates are like software bugs?

The industry has faulty standards, faulty engineering methods, faulty maintenance procedures, imperfect root cause analysis and incomplete corrective action. Over time these faults are exposed, identified and changes made to standards, designs or maintenance processes to eliminate or reduce the failure rate?

The paper goes on to note that failure rates level out but can never be zero. Is this the situation the aircraft industry is presently in? Where failures are now so unbelievable that the number of possibilities are too large to predict or manage? An example is the El Al cargo crash on 4/10/1992 where one engine broke loose from the wing, accelerated ahead of the aircraft, turned and collided with another engine knocking it off the wing.

✶ Risks of a flying society

<Nick Brown <Nick.BROWN@coe.int>>

Thu, 30 Aug 2007 14:30:50 +0200

I read with interest at <http://news.bbc.co.uk/1/hi/business/6970031.stm> that a company in Davis, California called Moller International is planning to sell, very soon, a personal flying machine, capable of hovering 10 feet off the ground, for about US\$90,000.

On visiting their site at <http://www.moller.com/> can discover

Moller's attitude to safety at <http://www.moller.com/safe.htm>. I didn't spend much time on this page; I'm sure that the safety of the pilot has been well thought-out. There's lots of redundant engine power, it can "land almost anywhere", the software is presumably highly reliable (!), and anyway, there's only 10 feet to fall, at least with the M200X model.

I found the most interesting aspect of the safety page to be the complete absence of any consideration of the 6-billion plus people who do not own or operate a "Skycar". Given that a large number of the initial owners will be rich people with bored teenagers in search of thrills and who may, on occasion, have access to mind-altering substances, I'll leave that as an exercise for the readers of RISKS.

To get the ball rolling: how many commercial premises currently consider that an eight-foot high chain link fence topped with a foot of razor wire, provides them with adequate security against intrusion?

Nick Brown, Strasbourg, France.

✶ Groklaw reports 'The Incredible "Lawyers as Hackers" Case'

<bo774@freenet.carleton.ca (Kelly Bert Manning)>

Fri, 24 Aug 2007 13:45:53 -0400 (EDT)

Many have commented that the Internet is like a shared long-term memory.

For practical purposes, it is impossible to retrieve or suppress anything once it has been posted on a webpage or in a news group. Individuals have been cautioned to assume that anything they post will be reviewed by future employers.

Enterprises should be aware that anything they post on a webpage can appear as evidence against them in court, and that measures they take to block archival of their webpages may fail and may not prevent use of the webpages as evidence.

This may seem obvious, but at least 1 USA enterprise went to some lengths to attack a legal firm which used printouts of archived copies of enterprise public webpages as evidence in court.

It seems bizarre that an enterprise could imagine that publicly accessible webpages could not be used as evidence in court cases, but Groklaw recently reported a decision where "Healthcare Advocates" did exactly that, claiming that accessing a webpage archive was "hacking" under the USA Digital Millennium Copyright Act, and that failing to preserve the content of a browser cache was "spoliating evidence".

The judge quoted their own expert witness as saying that automatic purging of expired cache data was normal browser behaviour, and was not evidence of any deliberate act by the defendant law firm.

✶EZ-pass evidence and the law

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

Mon, 3 Sep 2007 11:03:17 PDT

http://www.boston.com/news/nation/articles/2007/09/02/e_zpass_records_make_way_into_criminal_and_civil_trials/

E-ZPass records make way into criminal and civil trials;
They show where a vehicle traveled at a specific time
[Source: Madison Park, *Baltimore Sun*, 2 Sep 2007]

A woman accused of killing her husband was convicted after New Jersey prosecutors reconstructed her movements. Examining E-ZPass records, investigators pieced together the driving route of a missing Baltimore federal prosecutor who later turned up dead. Prosecutors in a New York City murder trial discredited a suspect's alibi.

[See also [RISKS-24.79](#).]

✶On-line property assessment databases a bit too accessible

<Jonathan Kamens <jik@kamens.brookline.ma.us>>

Sun, 09 Sep 2007 02:10:02 -0400

While engaged recently in a discussion with a parent at our children's school whom I felt was being overly paranoid about sharing her home address with other parents, I googled her name, suspecting that I would be able to illustrate to her that the information she was trying to protect was already

available on-line.

I succeeded far more than I'd expected to. One of the first matches returned by google was her home's property listing in the on-line property assessment database for the town of Arlington, Massachusetts, where she lives. Her name, her husband's name, their address, a picture of the house, a floor-plan sketch, the date they bought the house, their purchase price, and all of the information used by the town to calculate the assessed value of the house were instantly available.

Arlington's webmaster is guilty of two offenses: (1) providing an interface for searching the assessment database by name (i.e., if you go to <http://arlserver.town.arlington.ma.us/Property/>), you can search not only by address, but also by the owner's name); and (2) allowing its assessment database to be fully indexed by public search engines.

This is not a small thing. Consider a domestic abuse victim who moves to a new house in a new town to get away from her abuser. She takes precautions to avoid being tracked down, e.g., ordering telephone service in a fake name and paying the telephone company extra for an unlisted number. Unfortunately, however, the town she has moved to is Arlington, which proceeds to publish her name and address on its Web site for the world to see and search.

The discovery of Arlington's carelessness with its residents' privacy prompted me to check on Boston, where I live. Boston, too, allows its assessment database to be searched by name, but at least its

database isn't indexed in Google. Someone with nefarious intent trying to locate a Boston resident must already know that s/he owns a house in Boston. That's bad, but not as bad as Arlington.

I decided to check some other towns and cities in Massachusetts to see how they stack up.

I checked 61 towns and cities, of which only 9 had their data sufficiently secured (i.e., not easy to view the entire assessment database, not searchable by name, not searchable in Google). I found one town besides Arlington, Ashburnham, whose records were searchable in Google, and four towns (including Ashburnham) where it was easy to view the entire assessment database without needing to perform individual searches. In addition, I discovered that independent of town and city records, the registries of deeds of most Massachusetts counties allow their land records to be searched by name, most of them from a single, convenient Web site. See below for the details.

When assessment and land records were kept only on paper, they were organized by street name and number, not by owner name. When Massachusetts communities began to put these records on-line for public access, did they stop to think of the privacy, security and safety implications of allowing them to be searched by name? Apparently, only 9 of the 62 communities I looked at did, and most of them are probably in counties which didn't.

Is Massachusetts typical?

Jonathan Kamens

For those who are curious, here are the details of what I found:

* *Cambridge* - not searchable by name, not searchable in Google (PASS)

* *Abington* - * searchable by name, * *entire database can be viewed

by sending an empty search, * not searchable in Google (FAIL)

* *Adams* - *spreadsheet containing town's entire assessment database (last updated FY03) available on Web site, *not searchable in Google (FAIL)

* *Amesbury* - * searchable by name with free registration, * *entire

database can be viewed by sending an empty search, * not searchable

in Google (FAIL)

* *Amherst* - not searchable by name ("Owner Names are purposely not

a part of the search interface"), not searchable in Google (PASS)

* *Andover* - owner names don't appear in database (PASS)

* *Ashburnham* - database available as PDFs on Web site, *searchable

in Google* (FAIL)

* *Ashby* - *searchable by name, * not searchable in Google (FAIL)

* *Avon* - no on-line assessment database on-line, but links to*

Norfolk County Registry of Deeds whose database is searchable by

name for free, via "BROWNtech Document Management Systems"* (FAIL)

* *Acton, Acushnet, Agawam, Aquinnah, Ashfield, Auburn* - assessment

database doesn't appear to be on-line (PASS)

The discovery of the link to the Norfolk County Registry of Deeds on Avon's

Web site prompted me to check whether other counties' registries

are also
searchable by name.

* *Barnstable *- yes, via BROWNtech (FAIL)

* *Bristol-Fall River, Dukes, Franklin, Hampden, Hampshire,
Middle

Berkshire, Nantucket, North Berkshire, North Essex, North
Middlesex, North Worcester, South Berkshire, South Essex,
South

Middlesex, South Worcester, Suffolk *- yes, via
www.masslandrecords.com (FAIL)

Note that Abington and Amesbury both appear to use a third-party
service
called Vision Appraisal Technology (<http://www.visionappraisal.com/>) to host
their on-line assessment databases.

Ashby uses software hosted by the Community Software Consortium
(<http://csc-ma.us/>). This software also appears to be used by
Alford,
Ashland, Ayer, Bedford, Berkley, Bernardston, Bolton, Brookfield,
Charlemont, Chester, Duxbury, East Brookfield, Egremont,
Framingham, Gill,
Grafton, Great Barrington, Hardwick, Heath, Hingham, Holliston,
Lancaster,
Lee, Lunenburg, Mattapoissett, Maynard, Monroe, Needham, New
Braintree, North
Andover, North Brookfield, Northborough, North Reading, Oakham,
Richmond,
Royalston, Saugus, Seekonk, Sheffield, Somerset, Southborough,
Swansea,
Tolland, Uxbridge, West Brookfield, and Windsor, all of which
therefore
FAIL, and furthermore, there's a single convenient interface
that one could
use to easily search for a particular person by name in all of
these
communities.

✶ Police mail sensitive information to the press

<Debora Weber-Wulff <D.Weber-Wulff@fhtw-berlin.de>>

Sun, 09 Sep 2007 00:34:52 +0200

The German radio and television station SWR reports on September 7, 2007

<http://www.swr.de/nachrichten/bw/-/id=1622/nid=1622/did=2561310/1x2s3xt/index.html>

that police in Friedrichshafen (near Lake Constance) mistakenly sent secret information about their investigations of "terrorists" to their press mailing list by email.

The article says that they "recalled the mail" [no way of that happening, in my universe at least -dww]. The information included assessments of the current situation, lists of investigations and a list of endangered facilities. [just what your local terrorist needs -dww]

There will, of course, be a thorough investigation, someone will be fired or sent to do hard labor down in the cellars of the archives, or whatever it is that one is sentenced to if you are found to be the person guilty of making your superiors look like idiots.

The head of the police department apologized, but did note that perhaps this is just human error. [I think it is more likely a "helpful" email program, doing email-address completion. I've managed to send an email intended for my husband to a colleague (who discreetly destroyed it, thank goodness!) - dww].

Prof. Dr. Debora Weber-Wulff, FHTW Berlin, FB 4, Treskowallee 8,
10313 Berlin
GERMANY +49-30-5019-2320 [http://www.f4.fhtw-berlin.de/people/
weberwu/](http://www.f4.fhtw-berlin.de/people/weberwu/)

iTunes sharing

<Henry Baker <hbaker1@pipeline.com>>

Mon, 10 Sep 2007 12:12:54 -0700

With Bluetooth & WiFi enabled on your laptop, go to an airport
(or other
public place) & open up iTunes.

In many cases, you will see the sharable collections of tunes
from a number
of other people. It appears that this mechanism is completely
outside the
usual mechanisms of file sharing.

Even if you don't see any tunes, you still get to see various
computer
names. Since a number of people tend to name their laptops
after themselves
("Emily's PC", etc.), you can even find out their names.

Between the phones you see on Bluetooth, and the laptops you see
on WiFi,
you get a pretty good idea of who is around you, what kinds of
music/podcasts that they like, what kind of phone they use, etc.

I assume that this is intended to be some sort of ad hoc social
networking
scheme, but one that many people joined unconsciously.

Security: an example from Pakistan

<Dan Jacobson <jidanni at jidanni.org>>

Tue, 04 Sep 2007 05:43:02 +0800

<http://www.apdip.net/projects/igov/ICT4DSeries-iGov-Ch5.pdf>

The interlocking nature of technology and policy issues related to security are illustrated by the example of Pakistan. In 2000 the monopoly service provider had one point of entry and the international bandwidth was brought in via one undersea fibre with no redundancy. The ambition of the government to deploy pornographic content blocking on the core gateway router by putting up access control lists added to the vulnerability. The total bandwidth coming into Pakistan was less than 250 Mbps. Finally, the total lack of any security awareness and training in the staff manning the Internet Exchange set the stage for trouble. A childish exercise by Pakistan-based hackers to deface Indian sites was met by an equally immature response by the Indian hackers in devising the yaha virus. This was originally a Denial of Service (DoS) attack on all .gov sites. This rapidly escalated to a Distributed Denial of Service (DDoS) attack in different strains of the virus. This attack was accompanied by different varieties of attacks (fragmented packets, etc.) which coupled with the overloaded core router handling the pornographic access lists brought the complete network down. The attacks collapsed web servers, choked the domestic bandwidth, overloaded the router and consequently flooded the international

bandwidth. These attacks continued intermittently for several months as the Pakistanis tried desperately to address the multiple threats. The national network went down for hours and days at a time.

🔥 **Monster data capture also includes "USAJobs"**

<"Epstein, Jeremy" <Jeremy.Epstein@softwareag.com>>
Fri, 31 Aug 2007 17:02:05 -0400

The Monster hybrid attack (Infostealer.Monstres) has been discussed adequately [see [RISKS-24.81](#)]. What I haven't seen covered is that it apparently also affects anyone who applied for a US government job as well, according to an email my wife received from USAJOBS. According to that letter, "Monster Worldwide is the technology provider for the USAJOBS website and regrettably, some of the contact information captured came from USAJOBS job seekers. The information captured included name, address, telephone number, and email address. Monster Worldwide has assured the U.S. Office of Personnel Management that Social Security Numbers were NOT compromised because of IT security shields USAJOBS has in place."

I wonder how many other organizations "private label" Monster.com, and hence their customers are also at risk.

Redacted account numbers

<Tom Watson <sd695@yahoo.com>>

Mon, 3 Sep 2007 14:12:06 -0700 (PDT)

My bank (Wells Fargo) in its infinite wisdom has decided to change the way it attempts to redact account numbers. In looking over the transactions for an infrequently used account (I only have it because my ex-wife is a signer, and who knows when I'll need to cash a check with her name on it!) I noticed that the method had changed from the July to August automatic transfers I have to keep the account active. In July, the account number is listed with THE LAST 3 digits as 'X'. In August, the method is now all 'X' EXCEPT FOR THE LAST 4 digits. I just looked and said to myself "what is wrong with this picture?". The risk: when you change methods of redacting, change ALL occurrences, not just the new ones. You may just totally unredact what you were attempting to hide.

Fortunately in my case, I know the account number anyway, so TO ME it is no big deal (unless I print out something), but I'm aware, which is the the thing to be.

I sent the bank a note as well. I don't hold out much hope for anything constructive in return, but we will see.

[It seems pretty stupid to make such a change that completely exposes the account number to anyone with records before and after sanitization. PGN]

⚡ Re: Save your transaction numbers! (Koenig, [RISKS-24.80](#))

<Diomidis Spinellis <dds@aueb.gr>>

Fri, 24 Aug 2007 18:26:29 +0300

Andrew Koenig's story of a bank transaction he couldn't prove it occurred illustrates the need for keeping logs (including voting records) in a human-accessible format. I always print the transaction's final screen when I perform an electronic payment. I never analyzed why I needed to do that, it just seemed right to me. Banks, which have lot of experience in keeping track of money, keep a paper trail for all their transactions: they have me sign paper slips in duplicate at the teller, and even the ATM has a second printer in its housing logging all transactions on a paper roll. Reports regarding the demise of paper are greatly exaggerated.

Diomidis Spinellis - <http://www.dmst.aueb.gr/dds>

⚡ Re: Chinese Village Name Change Sparks Chaos ([RISKS-24.81](#))

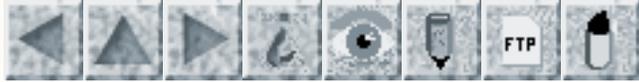
<Julian Bradfield <jcb@inf.ed.ac.uk>>

Thu, 30 Aug 2007 21:33:24 +0100

If the Wikipedia entry (Tianweiban) on this story is correct, the character isn't even particularly obscure - it's just not in the PRC simplified set. It is, however, in the standard Hong-Kong set

(Big5),

and used in Cantonese rather than Mandarin. There are vastly more obscure characters!



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 83

Thurs 27 September 2007

Contents

- [Air traffic radar and radio outage hits flights](#)
[Robert P. Schaefer](#)
- [Excel can't multiply](#)
[Steven M. Bellovin](#)
- [FIA blunder reveals secrets: obscured material viewable](#)
[Ben Moore](#)
- [Deploy first, test later](#)
[Steven M. Bellovin](#)
- [Redacted material still viewable](#)
[Ben Moore](#)
- [Fake blogs and search engines](#)
[Gadi Evron](#)
- [Silly "Bad Words" filter](#)
[Reinhard Kopka](#)
- [29th IEEE Symposium on Security and Privacy](#)
[Cipher Editor](#)
- [REVIEW: Endpoint Security, by Mark S. Kadrach](#)
[Richard Austin](#)

- [Eugene Miya <eugene@soe.ucsc.edu>](mailto:eugene@soe.ucsc.edu)
 - [Have you seen *Beautiful Code*? Awesome new book](#)
[Eugene Miya](#)
 - [Software Maintenance - A Management Perspective"](#)
[Phaneendranath](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Air traffic radar and radio outage hits flights

<"Robert P. Schaefer" <robert.p.schaefer@baesystems.com>>
Wed, 26 Sep 2007 12:36:41 -0400

A three-hour failure in three long-range air-traffic radar systems and radio communications in Memphis on 25 Sep 2007 caused the FAA immediate problems with 150 aircraft and subsequently affected perhaps 1000 planes in eight southeast/midwest states. Memphis-area regional controllers had to use their personal cell phones to contact controllers at other facilities. "The outage was the latest in a string of embarrassing air traffic control equipment and other problems this past spring and summer that spotlighted the aging system that handles thousands of flights daily." [Source: Reuters, 25 Sep 2007: PGN-ed]
<http://www.reuters.com/article/domesticNews/idUSN2541697920070925>

[Also noted by Ben Moore. PGN]

✶ Excel can't multiply

<"Steven M. Bellovin" <smb@cs.columbia.edu>>

Thu, 27 Sep 2007 15:51:12 +0000

According to a *NY Times* blog (Pogue's Posts), Excel 2007 for Windows doesn't cope properly when multiplying two numbers that should yield 65535 (<http://pogue.blogs.nytimes.com/2007/09/27/a-big-excel-boo-boo/>).

Instead, it gets 100,000.

For a very nice explanation and discussion of its relevance, see Joel Spolsky, Joel on Software blog <http://joelonsoftware.com/items/2007/09/26b.html>

✶ FIA blunder reveals secrets: obscured material viewable

<"Ben Moore" <ben.moore@juno.com>>

Tue, 25 Sep 2007 01:20:58 GMT

Sometimes redacting just isn't enough! Especially if you don't know what you're doing.

Formula-1's governing body has apparently blown of dozens more McLaren and Ferrari secrets. Technical and financial information in 200 pages of World Motor Sport Council transcripts had been redacted, but the blackened pdf text was of course easily copy-pasted and recovered. Although later removed from the website, the cat was out of the bag -- including technical team and car details, suspended McLaren chief designer Mike Coughlan's annual salary, the precise weight distribution of the MP4-22 and systems

adopted by
Ferrari, the "philosophy of variable brake balance systems on
both the
McLaren and the Ferrari", and details about Ferrari's unique
method of
inflating its tires.

[http://formula-1.updatestport.com/news/article/1190624301/
formula_one/F1headlines/FIA-blunder-reveals-secrets/view.html](http://formula-1.updatestport.com/news/article/1190624301/formula_one/F1headlines/FIA-blunder-reveals-secrets/view.html)

🔥 Deploy first, test later

<"Steven M. Bellovin" <smb@cs.columbia.edu>>

Tue, 25 Sep 2007 21:16:45 +0000

RISKS readers are familiar with the difficulty of deploying new
software
systems. Even with the best will in the world, some things with
just break.

In an effort to forestall this, Arizona State University decided
to act like

a 90s-style .com: deploy first, even if the software is buggy,
try to cope

with the problems, and fix the code later. As I read the Wall
Street

Journal story (for subscribers,

<http://online.wsj.com/article/SB119067729479838055.html>),

it didn't work very well. 3,000 employees were unpaid or
underpaid, and the

backup procedures couldn't scale by nearly enough.

Some of the trouble was that many employees in, say, janitorial
positions

didn't have their own computers, and not enough departmental
machines were

available. More of the trouble was the usual: the new system
didn't behave

the same way as the old one did, especially when handling minor
errors.

They had a backup plan: the HR department would write checks, no questions asked, for any employee who received an inaccurate paycheck. But there were too many errors, and HR couldn't keep up.

Mr. Reinke says instead of writing him a check to replace his blank paycheck, he was told that a change would be made in the system. He received his check a week later. In the meantime, he had to extend his overdraft protection in order to pay his \$800-a-month mortgage. Hundreds of other employees had to wait as many as 12 days to have their paychecks fixed. A spokesman for the Arizona State Credit Union says that 55 people took out short-term loans.

The new strategy's pain is undeniable. "Morale is the lowest it's been in the 14 years I've worked here," says Allan Crouch, who works in the university's human-resources department.

The university seems to be blaming HR, not IT. Two HR employees have been placed on leave. And the IT folks? They think the conversion was a success:

While unpaid employees may have been less than thrilled, school administrators, and consultants and software companies involved in the project rave about Arizona State's strategy. Oracle hailed it as a model for both universities and corporations to follow in a report it published in April 2007. In a statement, Jim McGlothlin, an Oracle vice president called the project "highly successful." Gary Somers, who

worked on the
project for CedarCrestone, Inc., the consulting company that
helped
implement the system, calls Arizona State's method "the wave
of the
future."

Ship first, debug later, use employees who haven't volunteered
for financial
hardship as your test subjects. Imagine the reaction of the
school's
Institutional Review Board if a professor has proposed a human
subjects
study with similar characteristics.

Steve Bellovin, <http://www.cs.columbia.edu/~smb>

⚡ Redacted material still viewable

<"Ben Moore" <ben.moore@juno.com>>
Tue, 25 Sep 2007 01:20:58 GMT

Sometimes redacting just isn't enough! Especially if you don't
know what
you're doing.

[Source: FIA blunder reveals secrets, 22 Sep 2007]
[http://formula-1.updatesport.com/news/article/1190624301/
formula_one/F1headlines/FIA-blunder-reveals-secrets/view.html](http://formula-1.updatesport.com/news/article/1190624301/formula_one/F1headlines/FIA-blunder-reveals-secrets/view.html)

With seemingly no end to the espionage saga, it now emerges that
F1's
governing body earlier this week contributed to the widespread
distribution
of dozens more McLaren and Ferrari secrets.

A day before releasing the nearly 200 pages of World Motor Sport
Council

transcripts to the public on Wednesday, the FIA had sent the documents to both teams so that confidential technical and financial information could be redacted.

But when the PDF documents were initially made available on the Internet, it soon became clear that the blackened sections could easily be revealed if copy-pasted into another text editor.

The offending copies were quickly removed from the FIA website and replaced.

But a plethora of sensitive information, including not only technical team and car details but private figures such as suspended McLaren chief designer Mike Coughlan's annual salary, and the precise weight distribution of the MP4-22 and also systems adopted by Ferrari, is therefore now widely known in various corners of the formula one world.

The philosophy of variable brake balance systems on both the McLaren and the Ferrari was also inadvertently revealed by the FIA, as well as details about Ferrari's unique method of inflating its tyres, and other secrets.

We can confirm that some of those in possession of the formerly private information have been approached by motor racing figures asking to be let in on the secrets.

An FIA spokeswoman admits that the Paris based Federation is aware of the mistake.

She would not comment further, but the FIA confirmed last week

that the transcripts had been recorded by a professional stenographer and formatted by an independent transcription company.

⚡ Fake blogs and search engines

<Gadi Evron <ge@linuxbox.org>>

Thu, 6 Sep 2007 01:06:13 -0500 (CDT)

URLs in this post should be considered as unsafe.

Fake sites and SE poisoning are nothing new. The use of blogs for this is far from new, either. Thousands of new fake blogs pop up every day on blogspot, livejournal, etc.

Web spam is a subject I have written about in the past, and some of you may be familiar with it regardless of me (no kidding), especially if you run a blog yourself.

A new fake blog which looks like blogspot, but has its own "domain", recently popped up in a Google alert on my name.

I get hits on these fake pages all the time as my name is a key word used by some of these spammers to grab attention to their pages. This time around they really over-did it.

The page has a blogspot layout, and continues with ads to pornographic sites or malware (is there any difference anymore?).

Then the site shows the YouTube video which can be found under

my name.

Following that is a post I made to a mailing list recently (poorly formatted). Then we have a few pictures of girls, linking once more either to pornographic sites or malware drive-by sites (if there is a difference, again).

They finish the page off by adding comments, which are actually some old securiteam posts by me.

Heck, it looks fake, but it is obvious the bad guys are investing more in their fake web pages. Their auto-creation tools seem to be getting more impressive, and I believe we will see much improved believable sites, soon.

Google Blog Search displays this site as (nasty words replaced with beep):

Gadi Evron
2 Sep 2007

[Text that would certainly tag this issue as s*p*a*m deleted by PGN]

URL:

<http://newadult.celeberia.com/Gadi-Evron>

Again, I am unsure if these URLs are safe.

For those of you wondering if these web pages mean anything to the bad guys, the answer is absolutely yes. Search engine ranking, indexing, etc. helps them advance their own sites (or their clients'). Then of course, there is advertising and Google ads. It works. And the advertising space on unrelated key words is a plus.

The concept is very similar to comment spam. Comment spam may not contribute to SE ranking anymore due to the nofollow tag attached to links in comments, but these get indexed and that's all the bad guys care about. Nofollow is crap, and what shows up when you search is what matters.

As an example of how these things work, in a recent blog post of mine a buddy left a comment (see here <http://gevron.livejournal.com/8859.html> for the example).

He left a URL for his legitimate Python/math/music/origami blog in his comment, and now when you search for his blog you find my post placed in the 4th place with the title 'A Jew in a German Camp' (about the CCC Camp in Germany). He is not pleased, but it is obvious how the bad guys abuse this, and infect millions of computers just because their owners surf the net.

✈️ Silly "Bad Words" filter

<Reinhard Kopka <kopka@gmx.de>>
Wed, 26 Sep 2007 15:31:44 +0200

On Wattflyer forum (for radio control eflight) a new filter was installed.

It turns words like 'class' into 'clear'. A list of bad words are changed against less offensive ones. Even word parts! So, for example, all occurrences of "ass" are changed into "rear". Just think of

grass, glass,
pass, embassy... <http://www.wattflyer.com/forums/showthread.php?t=24929>

It was deactivated after less than a day. Wonder why :-)

[Surprised that things like this keep happening? We're not.
PGN]

✦ 29th IEEE Symposium on Security and Privacy, Oakland California

<"Cipher Editor" <cipher-editor@ieee-security.org>>
Tue, 18 Sep 2007 10:39:57 -0600

Oakland 2008 29th IEEE Symposium on Security and Privacy,
The Claremont Resort, Berkeley/Oakland, California, USA, May 18-
21, 2008.

<http://www.ieee-security.org/TC/SP2008/oakland08.html>

(Submissions due 9 November 2007)

Since 1980, the IEEE Symposium on Security and Privacy has been the premier forum for the presentation of developments in computer security and electronic privacy, and for bringing together researchers and practitioners in the field. Previously unpublished papers offering novel research contributions in any aspect of computer security or electronic privacy are solicited for submission to the 2008 symposium. Papers may represent advances in the theory, design, implementation, analysis, or empirical evaluation of secure systems, either for general use or for specific application domains. The Symposium is also open to the submission of

co-located half-day or one-day workshops. Topics of particular interest

include, but are not limited to:

- Access control and audit
- Anonymity and pseudonymity
- Application-level security
- Biometrics
- Cryptographic protocols
- Database security
- Denial of service
- Distributed systems security
- Formal methods for security
- Information flow
- Intrusion detection and prevention
- Language-based security
- Malicious code prevention
- Network security
- Operating system security
- Peer-to-peer security
- Privacy
- Risk analysis
- Secure hardware and smartcards
- Security engineering
- Security policy
- User authentication

⚡ REVIEW: Endpoint Security, by Mark S. Kadrach (Richard Austin)

<"Cipher Editor" <cipher-editor@ieee-security.org>>

Tue, 18 Sep 2007 10:39:57 -0600

[Excerpt from Cipher Newsletter, IEEE CIPHER, Issue 80, September 17, 2007]

Endpoint Security, by Mark S. Kadrach Addison-Wesley 2007.
ISBN 0-32-143695-4 Amazon.com \$54.99 Bookpool.com \$29.95
Book Review By Richard Austin, 20 Jun 2007

Security professionals must face the fact that our networks are acquiring new types of endpoints at a frightening pace. They range from PDA's to smartphones to network-attached printers to even network manageable power strips. And, unfortunately, as Kadrich is quick to point out, these devices are all about features and functionality with little attention being focused on securing them before they attach themselves to our networks.

His second chapter, "Why Security Fails," provides an excellent summary of the reasons why security fails ranging from a check-the-box mentality ("if I do this, then I will be secure") to the fact that vendors always position themselves to stop the last threat (rather like the military is often criticized for planning to fight the last war).

Chapter 3 presents his idea of what is missing using the surprising analogy of the flush toilet and its control system. He points out that we need to approach the process of network security as a process control problem by identifying control points (routers, VPN gateways, etc) and establish control processes that integrate signals such as failed logon attempts, IDS alerts, etc and business processes such as user termination, software decommissioning and so on. He defines (yet another) new way of diagramming networks to reflect the control system analogy. While we need a new network diagramming standard like we need another compliance initiative, thinking about the denizens of our network infrastructures from a process control perspective is a source of useful insights.

Chapter 4 (Missing Link Discovered) introduces the proposed components of a solution that predictably includes network access control (NAC), But Kadrich also includes what is often the missing link in NAC decision making: host integrity. The basic concept is that a device must demonstrate a defined level of trustworthiness before it is allowed to join a more trusted part of the network. If the device cannot demonstrate integrity of its operating system, and a valid system configuration (anti-virus, firewall rules, etc), it will not be granted access. Additionally he makes the important point that the device needs to be remotely manageable so that remediation can be performed. For example, if a host is missing a critical patch as required by the integrity/configuration standards, it can be automatically installed as part of the NAC process.

The next two chapters flesh out the underlying components of the NAC process with a discussion of network capabilities and details on how to create a secure baseline for hosts.

In chapter 7 (Threat Vectors), the general ways an endpoint can be attacked are presented to prepare for a more in-depth look at threats and defenses for common software environments (Windows, OS X and Linux) in their own chapters. The chapter on OS X is especially recommended as security discussions of this increasingly popular operating system are rather rare.

Chapter 11 (PDAs and Smartphones) provides a good overview of

these very common endpoints and their software (Windows Mobile, Symbian, Palm, Blackberry and Mobile Linux). One could have wished for more detail but that would easily have doubled the size of the book and taken it further afield from its focus on endpoints in general.

Chapter 12 covers the important topic of embedded devices which include things ranging from a network-attached printer to the SCADA systems that run railyards and power plants. Kadrich notes that this is mainly an awareness chapter as there are almost no tools to implement anything approaching a NAC solution for them as yet.

The final chapter is devoted to brief case studies that illustrate the book's concepts and how they should be applied in practice.

In summary, "Endpoint Security" is a good overall look at the problems presented by the proliferating variety of endpoints seeking to attach to our network infrastructures. The presentation is concept-based which can be frustrating when one is seeking specific guidance but it more keeps the book from becoming mired in product details and quickly dated by their changing features. Practicing security professionals would be well advised to read the advice in this book and use it in examining just where the endpoints of their networks lie. If you're like me, you will find a few surprises along the way.

Richard Austin recently retired as the storage network security architect at

a Fortune 25 company and currently earns his bread and cheese as an itinerant university instructor and security consultant. He welcomes your thoughts and comments at rda7838@kennesaw.edu

🔥 Have you seen *Beautiful Code*? Awesome new book

<Eugene Miya <eugene@soe.ucsc.edu>>

Wed, 26 Sep 2007 14:20:53 -0700

%A Andy Oram

%A Greg Wilson, eds.

%T Beautiful Code

%I O'Reilly & Associates, Inc.

%C Sebastopol, CA 95472

%D 2007

%K book, text,

%X 1: Brian Kernighan, A Regular Expression Matcher

2: Karl Fogel, Subversion's Delta Editor: Interface As Ontology

3: Jon Bentley, The Most Beautiful Code I Never Wrote

4: Tim Bray, Finding Things

5: Elliotte Rusty Harold, Correct, Beautiful, Fast (in That Order):

Lessons from Designing XML Verifiers

6: Michael Feathers, Framework for Integrated Test: Beauty Through Fragility

7: Alberto Savoia, Beautiful Tests

8: Charles Petzold, On-the-Fly Code Generation for Image Processing

9: Douglas Crockford, Top Down Operator Precedence

10: Henry S. Warren, Jr., The Quest for an Accelerated Population Count

11: Ashish Gulhati, Secure Communication: The Technology Of Freedom

12: Lincoln Stein, Growing Beautiful Code in BioPerl

13: Jim Kent, The Design of the Gene Sorter

14: Jack Dongarra and Piotr Luszczek, How Elegant Code Evolves with Hardware:

- The Case of Gaussian Elimination
- 15: Adam Kolawa, The Long-Term Benefits of Beautiful Design
 - 16: Greg Kroah-Hartman, The Linux Kernel Driver Model:
The Benefits of Working Together
 - 17: Diomidis Spinellis, Another Level of Indirection
 - 18: Andrew Kuchling, Python's Dictionary Implementation:
Being All Things to All People
 - 19: Travis E. Oliphant, Multidimensional Iterators in NumPy
 - 20: Ronald Mak, A Highly Reliable Enterprise System for
NASA's Mars Rover Mission
 - 21: Rogerio Atem de Carvalho and Rafael Monnerat,
ERP5: Designing for Maximum Adaptability
 - 22: Bryan Cantrill, A Spoonful of Sewage
 - 23: Jeffrey Dean and Sanjay Ghemawat, Distributed Programming
with MapReduce
 - 24: Simon Peyton Jones, Beautiful Concurrency
 - 25: R. Kent Dybvig, Syntactic Abstraction: The syntax-case
Expander
 - 26: William R. Otte and Douglas C. Schmidt, Labor-Saving
Architecture:
An Object-Oriented Framework for Networked Software
 - 27: Andrew Patzer, Integrating Business Partners the RESTful Way
 - 28: Andreas Zeller, Beautiful Debugging
 - 29: Yukihiro Matsumoto, Treating Code As an Essay
 - 30: Arun Mehta, When a Button Is All That Connects You to the
World
 - 31: T. V. Raman, Emacspeak: The Complete Audio Desktop
 - 32: Laura Wingerd and Christopher Seiwald, Code in Motion
 - 33: Brian Hayes, Writing Programs for "The Book"
-

✶ Software Maintenance - A Management Perspective"

Phaneendranath

<phanee7@yahoo.com>

14 Sep 2007 15:32:37 -0700

Nearly 11 years after my Ph.D., the topic software maintenance is still hot

and demanding attention from management echelons. My thesis is now available in electronic format published by Universal Publishers. I thought you might be interested to check this at the link:
<http://www.universal-publishers.com/book.php?method=ISBN&book=1581129807>

Find out more about "Software Maintenance - A Management Perspective" by Vellanky, Phaneendra Nath at:
<http://www.upublish.com/book.php?method=ISBN&book=1581129807>

>From the abstract:

Computer systems play an important role in our society. Software drives those systems. Massive investments of time and resources are made in developing and implementing these systems. Maintenance is inevitable. It is hard and costly. Considerable resources are required to keep the systems active and dependable. We cannot maintain software unless maintainability characters are built into the products and processes. There is an urgent need to reinforce software development practices based on quality and reliability principles. Though maintenance is a mini development lifecycle, it has its own problems. Maintenance issues need corresponding tools and techniques to address them. Software professionals are key players in maintenance. While development is an art and science, maintenance is a craft. We need to develop maintenance personnel to master this craft. Technology impact is very high in systems world today. We can no longer conduct business in the way we did before. That calls for reengineering

systems and software. Even reengineered software needs maintenance, soon after its implementation. We have to take business knowledge, procedures, and data into the newly reengineered world. Software maintenance people can play an important role in this migration process. Software technology is moving into global and distributed networking environments. Client/server systems and object-orientation are on their way. Massively parallel processing systems and networking resources are changing database services into corporate data warehouses. Software engineering environments, rapid application development tools are changing the way we used to develop and maintain software. Software maintenance is moving from code maintenance to design maintenance, even onto specification maintenance. Modifications today are made at specification level, regenerating the software components, testing and integrating them with the system. Eventually software maintenance has to manage the evolution and evolutionary characteristics of software systems. Software professionals have to maintain not only the software, but the momentum of change in systems and software.

In this study, we observe various issues, tools and techniques, and the emerging trends in software technology with particular reference to maintenance. We are not searching for specific solutions. We are identifying issues and finding ways to manage them, live with them, and control their negative impact.

>From the acknowledgments:

If software development is an art, maintenance is craft. The nature of software maintenance and its study precludes originality. The practical nature of the field, the vast horizons that it covers, extensive product line - particularly hardware platforms, software, and applications, the experience with products, the budding tools and techniques, professionals entering almost from every other field and into various levels, makes software maintenance a peculiar field of study. This author draws inspiration and resources from his experience in software development and maintenance extending many years since 1972, and various courses and seminars attended on software maintenance, CASE Tools, Software Development Methodologies.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 84

Wednesday 3 October 2007

Contents

- [LAUSD payroll fiasco](#)
[David E. Ross](#)
- [Assessing personal risk](#)
[Jeremy Epstein](#)
- [Altered iPhones Freeze Up](#)
[Ken Knowlton](#)
- [Alameda e-voting results tossed out](#)
[Dave Leshner](#)
- [Dutch government suspends computer voting](#)
[Dik T. Winter](#) [Eric Ferguson](#)
- [Re: E-vote 'threat' to UK democracy](#)
[Blanche Kapustin](#)
- [Re: Memphis center outage](#)
[Bill Hopkins](#)
- [Re: On-line property assessment databases](#)
[Jonathan Kamens](#)
- [AOL classified RISKS-24.83 as spam](#)
[Ken Knowlton](#)

● [Re: Silly "Bad Words" filter](#)

[Gary Barnes](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ LAUSD payroll fiasco

<"David E. Ross" <david@rossde.com>>

Thu, 27 Sep 2007 16:56:28 -0700

Relating to Steve Bellovin's ``Deploy first, test later'' ([RISKS-24.83](#)), a

similar fiasco has been afflicting employees in the Los Angeles Unified School District (LAUSD) since early this year. LAUSD is the second largest K-12 public school system in the nation.

Some eight months after "going live" with their new payroll system,

employees are still receiving incorrect paychecks or no paychecks at all.

The administration does not yet know whether correct W2 forms will be issued in January. Employees retiring cannot get correct pension benefits.

Of course, when the new system was deployed, there were no contingency plans to roll back to the prior system. By now (after a delay of months), a roll-back is likely to be impossible.

David E. Ross <<http://www.rossde.com/>>

[On 1 Oct 2007, an NPR report mentioned that Deloitte Touche had received

\$95M for the original system, which did not work, and that another \$10M

had been spent on contracts aimed at fixing the system --

which to date
still does not work. PGN]

✚ Assessing personal risk

<"Epstein, Jeremy" <Jeremy.Epstein@softwareag.com>>
Fri, 28 Sep 2007 15:32:41 -0400

I haven't seen this talked about, although there have been a few blog comments. A Sep 24 article in **The Washington Post** summarizes research done by Dr. Jennifer Lerner at Carnegie Mellon on individual perceptions of risk. Not surprisingly to readers of RISKs, people dramatically misjudge risk - but what was surprising to me is how they did it in contradictory ways. WashPost says "Lerner found that anger and fear systematically bias people's risk estimates in opposite directions. Anger causes people to underestimate risks, which may be why drivers in the grip of road rage confidently attempt perilous maneuvers that place themselves and others in danger. By contrast, people who are afraid overestimate risks."

The **WashPost** article also discusses research by psychologist David Mandel of Defense Research and Development Canada, noting "While psychology is not much use in predicting the future when it comes to terrorism, what it can do is highlight errors in thinking. Mandel asked people after the Sept. 11 attacks what they thought the risk of a major terrorist attack would be in

the next two months. He then asked his volunteers to estimate the risk of an attack specifically by al-Qaeda and the risk of an attack by a completely separate group. Mandel found that when he totaled a person's responses about the likelihood of each of the subdivided possibilities, their sum was greater than the person's guess about the overall likelihood of a terrorist attack." Also, people misconstrue their own risk vs. the risk to others: "People invariably see themselves as being at lower risk than the average person -- they guessed that they had a 1-in-5 chance of being hurt but that others had a 1-in-2 chance of being hurt. Obviously, these statistics cannot be true for everyone."

So to bring this back to RISKS, I wonder how these psychological results apply to technology risks. Do we underestimate the risk of cyberattacks and take unnecessary risks (e.g., knowingly going to dangerous web sites, not running the latest security software) because we think we're immune as security professionals? Or are we overestimating our risk because we're afraid? I don't have any answers, but the article made me think about risks and RISKS.

<http://www.washingtonpost.com/wp-dyn/content/article/2007/09/23/AR2007092300915.html>

Altered iPhones Freeze Up

<Ken Knowlton <KCKnowlton@aol.com>>

Sat, 29 Sep 2007 09:38:51 EDT

A software update to Apple's iPhone on Friday disabled third-party applications and rendered iPhones that had been unlocked completely unusable. [Source: Katie Hafner, *The New York Times*, 29 Sep 2007]

<http://www.nytimes.com/2007/09/29/technology/29iphone.html?th&emc=th>

⚡ Alameda e-voting results tossed out

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

Tue, 2 Oct 2007 14:05:51 PDT

Judge Voids Election Results Over E-Voting Results That Couldn't Be Audited

Apparently a judge in Alameda County, California, has voided some election results after the e-voting tallies from Diebold machines couldn't be audited. The vote was on a controversial ballot measure, where the end result was quite close. [Source: Techdirt, 2 Oct 2007, thanks to Dave Leshner]

<http://techdirt.com/articles/20070930/001319.shtml>

⚡ Dutch government suspends computer voting

<Dik.Winter@cwi.nl (Dik T. Winter)>

Sat, 29 Sep 2007 02:06:38 GMT

On 28 Sep 2007 the Dutch government suspended all voting by voting machines.

In a report it was found that the systems were unsafe, not controllable and did not allow recounting. So while most of the country had converted to

voting computers, the next vote will again be with a red pencil. (Amsterdam

was late in conversion, so I only voted once with a machine, but that

machine was already disallowed on the next vote, so we got back to pencil

early.) The major problems seen are:

1. There is no way to verify that a machine runs a version of the

software that is approved.

2. There is no way to recount if there is a dispute.

The recommendation of the commission that looked into it is to wait for

voting machines that print out a paper recording the vote that you put in a

box. When counting starts, the papers from the box are collected and

another machine does the counting. This indeed would reduce a lot of paper

work (I have had A2 format forms where I should make one circle red). And

there is a clear paper trail, so if a counting machine is not trusted,

counting by hand is always possible.

I think the recommendations are pretty risk-aware, let the machines do what

they can do, but leave a full controllable trail.

Aside: the size of the voting papers is because almost all elections include

fifteen to twenty parties, with up to 50 persons on the list.

And you have

to choose one of those.

And, PS, it is rumoured that the producer of the Dutch voting machines (or one of its employees) has edited the Wikipedia page.

And finally, Amsterdam (with red pencil voting) had its final results long before other communities that did use computer voting on the last vote.

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

⚡ Dutch government suspends computer voting

<"Eric Ferguson" <e.ferguson@antenna.nl>>
Sat, 29 Sep 2007 01:40:50 +0200

[...] The whole issue of voting machines will be reconsidered from scratch.

Look at "www.WijVertrouwenStemcomputersNiet.nl" for more information, or look at government sources or newspapers like www.nrc.nl and www.trouw.nl, with the search term "stemcomputers" and "nedap".

Eric T. Ferguson, van Reenenweg 3, 3702 SB ZEIST Netherlands tel 030-2673638

⚡ Re: E-vote 'threat' to UK democracy (Leshar, [RISKS-24.71](#))

<Blanche Kapustin <info@blanchekapustin.com>>

Sun, 30 Sep 2007 04:07:19 +0200

I noticed I was quoted in [RISKS-24.71](#), and thought you might want an update.

The BBC interview seems like ages ago, but it was just before the last presidential election.

First, the laws have since changed and all of our state of Virginia is looking into new machines. I've only heard bits of this, but I suspect we'll all hear much more in the coming months.

Second, I'm not "the election official." I'm a seasonal employee at the Office of Elections. There are plenty of people who know more about election machines, e-voting, laws, and elections in general than me. They are full-time staff at the Office of Elections.

Third, most of the reporters who interviewed us that day got their facts wrong. For starters, have you ever heard an American say "tick" in this context? We say "check" or "checkmark." One newspaper stated my name as Miss Blanche Kapustin, right next to a photo of my hand on the machine's screen, displaying my wedding ring. Some misspelled my name. And many took bits and pieces of what we said and twisted it out of context. For example, one neglected the word "not" in a sentence. That totally changed the meaning.

In any case, if you have any questions, feel free to e-mail me at info@blanchekapustin.com. But please disregard anything you read in the

press. It's outdated, but even at the time, most of it was obviously misquoted.

✶ Re: Memphis center outage ([RISKS-24.83](#))

<"Bill Hopkins" <whopkins@wmi.com>>

Fri, 28 Sep 2007 18:31:58 -0400

It appears that the only failure in Memphis was the comprehensive communication system, which appears to put a lot of eggs in one somewhat fragile basket.

In the olden days, there were separate redundant sets of comm lines for

- receiving radar reports from the sensors,
- co-ordinating with other facilities, and
- talking to the aircraft.

If the radar lines went down, center could still talk to the pilots and the next center.

FTI, the Federal Telecommunications Infrastructure program, replaces all of these with a single, demonstrably-not-sufficiently-redundant pipe. It seems to have been taken down by a single board failure.

Insert appropriate jumping-up-and-down here. Oh, I may have left an 'r' out of the subject line.

For the technician's union take, see

http://www.newsmgr.com/publish/article_911.shtml

✈ **Re: On-line property assessment databases ([RISKS-24.82](#))**

<"Jonathan Kamens" <jik@kamens.brookline.ma.us>>

Mon, 24 Sep 2007 12:42:01 -0400

I have received a number of enlightening responses to my submission about on-line property assessment databases in [RISKS 24.82](#). I would like to share these and my responses to them in turn.

One respondent disputed my claim that before these databases were put on-line, the corresponding paper records were indexed by address rather than name. He wrote, "I don't think that is precisely true with respect to the land records. Deeds are indexed by grantor/grantee, not by street name/number."

I may have been mistaken in my belief that paper records were not indexed by grantee. However, I submit that it's rather easier for someone with nefarious intent to sit in front of a computer for an hour searching registries on-line than for him/her to travel in person to registries of deeds all over the state / country and start pulling books off the shelf to find someone.

Yes, the information was always public (a point made by other respondents), but it was not always so easy for the public to gain access to it. The information can and should be sufficiently accessible for people who have a real, legitimate need to access it, but it should at the same time be sufficiently **in**accessible to dissuade people

whose need is
not legitimate.

**

Another respondent asked if I knew about www.zabasearch.com and www.intelius.com, both of which (along with others, I'm sure) "provide lots of name-based info derived from public records." I am indeed familiar with these services, although I haven't ever paid them money to find out just how much information they are able to uncover. As my respondent noted, the information they provide is derived from public records, so this goes back to the issue which prompted my initial submission to RISKS -- the level of information available in the public records is itself a concern.

**

On a related note, one respondent noted that there numerous companies which have made a business out of sending ``data moles'' in person to registries and other government offices to grovel through paper records and capture their contents into private databases which can then be used and sold for various purposes (e.g., I've received numerous solicitations which identify the amount of my existing mortgage and the lien holder, and I recently received an official-looking letter offering to provide me with a registered copy of my deed (which of course I already have) for \$60). He reasoned that since these databases already exist and are accessible for a fee, it's reasonable for the government offices to make the data available themselves for free, to ensure equal access to it.

I see two flaws in this argument:

1. It presupposes that we should in fact be allowing private companies to collect and disseminate the data. Perhaps the right answer is not to allow everyone to access it since these private companies already are, but rather to restrict access for these private companies as well. It seems to me that it would be virtually impossible for such companies to do business in Europe, given the strict privacy laws there. With identity theft such a huge problem nowadays, it is not obvious to me that the European model isn't closer to correct than ours.

2. These private companies don't give away the data for free; they're doing the data collection to make money from it, so they charge for it, and even a minimal fee for access is a decent barrier for dissuading casual use of the data for nefarious purposes. It may in fact be perfectly reasonable to allow third-party databases of this data to exist (although, as noted above, that's an open question), as long as there are such barriers.

In my opinion, the data in land and assessment records should be freely accessible on the Internet without any names associated with it. If you want to look something up by name, there needs to be some sort of barrier to doing that, although I don't have a firm opinion about the nature or height of the barrier. Some possibilities include fee-based access; appearance in person at the registry; and being required to show cause for such a look-up

assuming that it isn't for your own data.

**

Two respondents mentioned Florida's Sunshine Law, which requires the vast majority of government information to be public and accessible. While I understand and to some extent agree with the motivation behind this law, even this law has exceptions to address safety and privacy concerns, and I would argue that being able to search land records by name should be such an exception.

Tanner Andrews, a lawyer from Florida, expounded at length about why the information which concerns me should be public. Most of the points he made in his response are irrelevant to my point, since they do not depend on the information being searchable by name, and thus do not contradict my claim that whatever minimal benefit there might be from such searchability is outweighed by the risk. The closest that Mr. Andrews came to explaining why the database should be searchable by name was this:

"Here in Florida, most of the property appraisers are elected. If you suspect some partiality, you ought to be able to see what property is owned by the people who gave the statutory maximum to the campaign. You ought as well to be able to decide whether those properties appear to be especially favorably assessed. In areas where the appraiser is appointed you may wish to do a similar investigation of properties owned by the people doing the appointing."

I do not find this argument convincing, because the reality is that the people doing such investigations are not private citizens but rather public advocates, journalists, etc. These people have the time and resources to find out where "the people who gave the statutory maximum" and "the people doing the appointing" live. Once you know where these people live, you can look up their property values by address, which I've never argued should be impossible. Please see my earlier point about making the information both sufficiently accessible and sufficiently inaccessible.

Mr. Andrews also wrote:

"Furthermore, a dedicated stalker can do the same things for the lady of his misguided affections. The computer search may save him the half-hour in the Clerk's office, but someone who has time to stalk probably has time to visit the courthouse as well."

This is true if a stalker already knows the town or city in which his/her target resides. However, as I've noted previously, the ease of access to these data on-line makes it possible for someone with nefarious intent to search, quickly, easily and for free, not just a single town or city, but an entire state or indeed multiple states. This is hardly comparable to the example Mr. Andrews gave of a "half-hour in the Clerk's office."

**

Another respondent mentioned the possibility of keeping one's name out of land records by assigning the property to a trust rather than to individual owner(s). Trusts are complex legal instruments that cost money to establish, and I hardly think that individual property owners should be burdened with that expense just to keep their names out of on-line property databases. Furthermore, the task of educating at-risk individuals of the need to utilize such trusts to conceal their location is a daunting one.

**

Finally, one respondent informed me that California has legislation prohibiting the public dissemination of property records with owner names. I have not been able to verify this, but if it's true, then it indicates that at least one state understands this problem and has taken steps to deal with it. It's not surprising that it's California; they frequently lead on things like this.

AOL classified [RISKS-24.83](#) as spam

<Ken Knowlton <KCKnowlton@aol.com>>

Fri, 28 Sep 2007 18:29:09 EDT

[Fortunately, Ken caught it. Maybe it was the "silly bad words" item?

But AOL already had a bad rep for rejecting all sorts of good content.

PGN]

✉ Re: Silly "Bad Words" filter (Kopka, [RISKS-24.73](#))

<Gary Barnes <gkb@adminsputting.org>>

Thu, 27 Sep 2007 23:29:35 +0100

Reinhard Kopka wrote of a "bad words" filter that triggered on partial word matches and replaced the partial match with a cleaner alternative.

In a similar vein, the facility to talk with other players at your table on Partypoker.com triggers on a part of an innocent word partially matching a rude word, and so changes "full house" to "YYYY house", which would seem to be a little overzealous.

[NOTE: Two out of four letters matching an offensive four-letter word?

That really is overzealous. By the way, I changed the four Xs to four Ys

in an attempt to avoid spam-filtering of *this* issue! 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

Search RISKS using [swish-e](#)

Volume 24: Issue 85

Thursday 11 October 2007

Contents

- [DHS List Server causes flood](#)
[David Lesher](#)
- [LI Railroad double-bills for tickets](#)
[Al Stangenberger](#)
- [California off the Net](#)
[Bryan Webb](#)
- [Clues to 3 Plane Wrecks Could Be Lost in Files Purge](#)
[Ken Knowlton](#)
- [Name hacking comic strip](#)
[Anders Sandberg](#)
- [Another case of Deploy First, Test Later](#)
[Huge](#)
- [Stalling Cars Via OnStar: A Hacker's Dream Come True?](#)
[Lauren Weinstein](#)
- [Microsoft HealthVault and Porn](#)
[Lauren Weinstein](#)
- [The Coax Straightjacket: Stopping Cable Copy-Protection Abuse](#)
[Lauren Weinstein](#)

- [Proposal for Breaking the Internet Network Neutrality Deadlock](#)
[Lauren Weinstein](#)
 - [Practical Issues of the Proposed "Global Internet Measurement Analysis Array"](#)
[Lauren Weinstein](#)
 - [More Regarding the Online Medical Records Trap](#)
[Lauren Weinstein](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ DHS List Server causes flood

<"David Leshner" <wb8foz@panix.com>>
Thu, 4 Oct 2007 19:35:07 -0400 (EDT)

It started off early Wednesday as an innocuous request from a North Carolina businessman to the Homeland Security Department. He was responding to a daily antiterrorism bulletin by asking that it be sent to another e-mail address. But by afternoon, a programming flaw involving the REPLY function transformed that e-mail message into a flood of more than 2.2 million messages nationwide that clogged the e-mail accounts of government and private experts on domestic security, including the operators of an Illinois nuclear power station. [Source: Eric Lipton, Security Bulletin Problem Creates Message Flood, *The New York Times*, 4 Oct 2007]
<http://www.nytimes.com/2007/10/04/us/04secure.html>

[Who needs a greater-than-3-oz liquid bottle when an e-mail reply will do?

Do we need to get DHS a new broom and bucket to clean up this mess?

Clearly they (or more likely the contractors they hired...) need a senior

sorcerer to watch over the apprentice admins.]

[See also Lauren Weinstein's blog on this topic, Homeland Security Floods

Users With Private E-Mail. PGN]

<http://lauren.vortex.com/archive/000305.html>

LI Railroad double-bills for tickets

<Al Stangenberger <forags@nature.berkeley.edu>>

Tue, 09 Oct 2007 12:13:15 -0700

At least 2,000 Long Island Railroad passengers were double-billed for tickets purchased with credit cards at automatic ticket kiosks in early October. The problem occurred on the first business day in October. A record number (over 30,000) of tickets were purchased by credit card via their network of automated kiosks. This triggered a software error (apparently undetected since 2001) which caused the system to bill for the tickets on October 1, and then again on October 2. The vendor is working on the problem. [It's not clear from the article whether the problem is in each of the 269 kiosks, or possibly some central server.]

[Source: Michael Amon, *Newsday*, 5 Oct 2007]

<http://www.newsday.com/news/local/ny-lilirr1006,0,7787106.story>

California off the Net

<"Bryan Webb" <bwebb@optivus.com>>

Fri, 5 Oct 2007 17:51:54 -0700

You are responsible for a sub-domain of a large, distributed, and well-known organization. Your DNS server, maintained by your ISP, gets hacked so that its entries are pointing to pornographic websites. When your ISP doesn't resolve the issue after 2 weeks, you switch to another DNS provider and fix the problem.

In the meantime, someone has discovered the problem, but suspects it is not just your domain that's been hacked, but your entire organization's, and complains to your new DNS provider. They, of course, don't recognize your well-known DNS name, nor try to effectively resolve the issue. As a result, you and all your sister domains are erased from the net.

And that's how the General Services Administration came to remove California's ca.gov domain -- because your domain tam.ca.gov was hacked.

(That's the Transportation Authority of Marin county.)

<http://www.networkworld.com/news/2007/100407-feds-pull-ca-gov-domain.html>

Talk about Denial of Service!

[*NYT* item noted by David Leshner.

http://mobile.nytimes.com/2007/10/05/us/05brfs-APOLOGYAFTER_BRF.xml

PGN]

✦ Clues to 3 Plane Wrecks Could Be Lost in Files Purge

<KCKnowlton@aol.com>

Thu, 4 Oct 2007 09:25:29 EDT

The Air Force destroyed all records from unsuccessful searches for aircraft missing before 1989, which is likely to make it much harder for Nevada investigators to determine the victims of three wrecks found in the recent search for the aviator Steve Fossett ... One resource that had been expected to help in the inquiry was suspended mission files, kept at Tyndall Air Force Base in Panama City, Fla. Those files are the paper trails of all failed searches for missing aircraft by the Civil Air Patrol, a volunteer Air Force auxiliary group, or any other Air Force resources. But in 1994, the Air Force instituted a regulation requiring the destruction of records of noncombat missions after seven years. [Source: Steve Friess, *The New York Times**, 4 Oct 2007; PGN-ed]

<http://www.nytimes.com/2007/10/04/us/04fossett.html?th&emc=th>

✦ Name hacking comic strip

<"Anders Sandberg" <asa@nada.kth.se>>

Wed, 10 Oct 2007 11:05:50 +0200 (MEST)

A cartoon with a cute exploit:

<http://xkcd.com/327/>

This example may not work in real life due to naming laws, but I

would be surprised if there were some systems out there vulnerable to names with exotic letters being interpreted as escape characters.

Anders Sandberg, Oxford Uehiro Centre for Practical Ethics,
Philosophy Faculty of Oxford University

[xkcd is "A webcomic of romance, sarcasm, math, and language".
This item was also noted by John Tate. PGN]

✈ Another case of Deploy First, Test Later (Re: Ross, [RISKS-24.84](#))

<Huge <huge@huge.org.uk>>
Wed, 10 Oct 2007 15:00:03 +0100

Many years ago, I was involved in 'porting' the payroll system of a large British TV company from an ICL 1902S to an ICL 2903 (told you it was a long time ago). We actually rewrote the whole thing in RPG2, from its original Autocoder. We moved the data between the two machines on punched cards.

So, come the day of the first parallel run, after months of testing, and the results were different. Not much, a few pennies, but different nonetheless.

Huge panic, much headless chicken behaviour until we discovered that ... the old system was the one that was wrong. And had been for years.

So, what have we learned in the intervening 30 years? Not a whole lot, it appears.

✂ Stalling Cars Via OnStar: A Hacker's Dream Come True?

<Lauren Weinstein <lauren@vortex.com>>

Tue, 09 Oct 2007 12:05:41 -0700

<http://lauren.vortex.com/archive/000313.html>

Ready to turn over the keys of your vehicle to the cops, or that clever hacker in the next lane? How about that creepy guy following you on a lonely country road?

GM apparently plans to perhaps make this all possible. It's been announced that they'll be equipping nearly two million of their 2009 model vehicles (that have OnStar installed), with the capability to be remotely shut down to idle via OnStar commands at the request of law enforcement (<http://abcnews.go.com/Business/Autos/story?id=3706113>).

The claim is that owners will have to give permission first for this capability to be enabled. Bull. I don't care what OnStar's privacy policy says, if the technical capability for this function is present, OnStar will have no practical choice but to comply when faced with a law enforcement demand or court order, whether or not owner "permission" was ever granted.

This new capability will also create an irresistible challenge to the hacker community -- and perhaps criminal organizations -- to try find ways into the OnStar system for triggering this fun -- one way or another. It's

impossible to hack OnStar? Would you bet your life on that?

Unfortunately, this is yet another laudable idea that's being "driven" into the marketplace before all of the negative ramifications have been thought through or fully understood. And how long will it be before such systems are mandated, one might wonder?

OnStar has long been the subject of various privacy concerns. This new capability appears to be the most serious privacy-related issue for OnStar to date.

Lauren Weinstein lauren@vortex.com or lauren@pfir.org +1 (818) 225-2800

Lauren's Blog: <http://lauren.vortex.com> PRIVACY Forum: <http://www.vortex.com>

Microsoft HealthVault and Porn

<Lauren Weinstein <lauren@vortex.com>>

Tue, 09 Oct 2007 09:39:48 -0700

<http://lauren.vortex.com/archive/000312.html>

It looks as if Microsoft may already have some significant quality problems with their heavily hyped HealthVault.

I received an e-mail last night from a reader who was disgusted to find that some completely valid queries to the HealthVault search engine -- mentioning bodily parts or bodily functions -- returned extremely high percentages

(sometimes almost 100%) of porn keyword "sucker" pages (porn pages that have been "seeded" with all manner of likely keywords). I won't offer example search strings here in the interests of good taste, but I've confirmed this situation myself.

In fact, this person noted getting masses of porn results starting with their very first HealthVault search. They were stunned that Microsoft's quality control and presumed filtering of results for health relevance were so defective on a highly touted health-specific search engine deployed for the general public. I agree.

For comparison purposes, a test of the same searches on Google also yielded a lot of porn hits, but overall more relevant hits were returned, and Google isn't promoting their main search engine as having a health focus.

There is a potential bright side to this situation. I'm all in favor of using encryption whenever possible on the Net, and HealthVault uses SSL crypto for searches in both directions. So finally there's a way to search for porn on the Net with better privacy!

All Microsoft needs to do now is simply rebrand their service as "PornVault" -- now that's a winner.

Lauren Weinstein lauren@vortex.com or lauren@pfir.org +1 (818) 225-2800

Lauren's Blog: <http://lauren.vortex.com> PRIVACY Forum: <http://www.vortex.com>

✶ The Coax Straightjacket: Stopping Cable Copy-Protection Abuse

<Lauren Weinstein <lauren@vortex.com>>

Mon, 08 Oct 2007 16:08:46 -0700

<http://lauren.vortex.com/archive/000310.html>

VHS is dead. Its ghost lingers in our homes and in cobweb-filled corners of electronics retailers, but make no mistake, VHS recording is rapidly going the way of the dodo. And this passing is being used as an excuse for one of the biggest consumer ripoffs in technology history -- with our friendly neighborhood cable television services (in their various incarnations) chuckling mightily at the situation.

When we first started hearing about Digital Rights Management (DRM) systems planned for digital television, there was a great deal of concern, even though the planned focus appeared to be on "premium" programming (HBO, Showtime, Pay Per View - PPV, and so on). Much of this seemed rather academic anyway, since consumer devices that would be affected by such systems were still largely vaporware.

But that situation has changed rapidly, and now cable firms (and their fiber, satellite, IPTV, and other variations -- I'm calling them all cable) have got their subscribers by the you know what, and unless the FCC (fat chance) or Congress (perhaps a better chance) get moving, consumers will see their hard won rights to record and save television programming

fade into
history. It's happening right now.

The Supreme Court "Betamax" decision decades ago established the fair use rights of consumers to make copies of television programs, and save them on videocassettes. But with the demise of VHS, the newly ascendant technology is Digital Video Recorders (DVRs), such as the TiVo and its various cruder generic cousins (the latter typically cable company supplied).

DVRs allow saving of programs on their internal hard drives, but there's a problem. Video takes a lot of bits, and hard drive space is limited. So the trend now is to find ways for consumers to save programs to external media and devices (such as DVDs or PCs), much as they could with VHS tapes.

Direct DVD recorders are appearing, as are newer generation TiVos that will shortly have the capability enabled to move programs to PCs and then write them to DVDs.

But many cable firms are trying to thwart these capabilities via DRM, trying to turn back the clock to pre-Betamax days. Their magic wand for this purpose is the Copy Control Information (CCI) byte, transmitted as part of digital cable channels, which impacts any modern device that interfaces directly to a cable system (e.g., through cableCARDS like with the newest TiVo HD -- and many more devices so affected are now appearing).

Set CCI=0x00, and the consumer can dump programs off of their DVRs. Set it to 0x02, and the programs are locked down. The device manufacturers must

abide by this rule or suffer the wrath of CableLabs -- the cable industry's own version of Dr. Evil's R&D operation.

Given the power that CCI holds over consumers, one would think that there

would be concise standards for how it would be applied to programming.

Buzzz! Wrong! In fact, the significant regulations that apply to CCI

simply require that digital broadcast channels (that is, over-the-air

signals retransmitted as digital cable channels), must set

CCI=0x00. Beyond

that, the regs are essentially silent.

Now, logically one wouldn't be surprised to find cable companies setting

CCI=0x02 -- blocking program saving to DVDs, etc. -- for special event

programming, PPV, and perhaps even the HBO/Showtime class of premium

channels.

What you might not expect to frequently find is cable company ad hoc CCI

blocking of essentially *all* basic digital channels (other than over-the-air) totally on their own volition -- creating unfair

recording

capability variations around the country.

For example, Time Warner Cable is generally setting CCI=0x02, and blocking

dumping of programs from DVRs, in this expansive manner.

There's no

evidence that all of these programs suppliers have demanded such an action.

Many of these channels run Cable in the Classroom programming that is

specifically licensed to be recorded, saved, and distributed in schools

under various terms. CCI=0x02 can directly block such licensed use.

Similarly, it seems unlikely that the various C-SPAN channels would demand blocking of program dump functions, yet Time Warner is routinely setting CCI=0x02 for some or all of these channels as well (which may often appear only on digital tiers) on many TW systems.

Since nothing requires TW to be taking this broad control freak approach to DRM on their digital channels, the most likely explanation would seem to be a CYA mentality run amok, subscribers' rights be damned.

Comcast, on the other hand, has reportedly been trending in the opposite direction, with their systems moving toward CCI=0x00 settings for most digital channels, allowing consumer program dumping and external saving.

Question: What possible valid reason can there be for cable subscribers of one company's systems to have vastly fewer recording rights for the same channels, compared with subscribers of another company's cable systems?

Answer: There's **no** valid explanation for this disparity. It's wacky, wrong, and just plain unacceptable. And as more consumer devices affected by this craziness rapidly deploy in the marketplace, subscribers are going to go ballistic when they discover that the pricey boxes they've bought have key functionality cut off at the knees by cable company edict in many locations.

If the cable industry was smart, they'd collectively start reversing draconian CCI settings right now, and start universally treating

their subscribers as individuals to be appreciated, not chattel to be abused. But absent such an enlightened approach from the industry as a whole, it's likely that we're going to have to make it clear to Congress that when it comes to this sort of DRM abuse (to paraphrase Howard Beale in the 1976 film "Network"): "We're as mad as hell and we're not going to take this anymore!" -- assuming that our cable companies don't try to block this too, of course.

Lauren Weinstein lauren@vortex.com or lauren@pfir.org +1 (818) 225-2800

Lauren's Blog: <http://lauren.vortex.com> PRIVACY Forum: <http://www.vortex.com>

🔥 Proposal for Breaking the Internet Network Neutrality Deadlock

<Lauren Weinstein <lauren@vortex.com>>

Thu, 27 Sep 2007 14:55:42 -0700

I've just posted a proposal for a project aimed at moving past the current Network Neutrality impasse, with the deployment of a distributed global Internet traffic measurement system as a major component.

<http://lauren.vortex.com/archive/000299.html>

Comments, questions, etc. are welcome. Thanks!

Breaking the Internet Network Neutrality Deadlock (HTML)

<http://www.pfir.org/nn-proposal>

Breaking the Internet Network Neutrality Deadlock (PDF)

<http://www.pfir.org/nn-proposal.pdf>

Lauren Weinstein, +1 (818) 225-2800 <http://www.pfir.org/lauren>
Lauren's Blog: <http://lauren.vortex.com>

✈ Practical Issues of the Proposed "Global Internet Measurement Analysis Array"

<Lauren Weinstein <lauren@vortex.com>>

Mon, 1 Oct 2007 15:08:32 -0700 (PDT)

Practical Issues of the Proposed
"Global Internet Measurement Analysis Array"
<http://lauren.vortex.com/archive/000303.html>

In "Proposal for Breaking the Internet Network Neutrality Deadlock" (<http://lauren.vortex.com/archive/000299.html>), I recently suggested a project for the gathering and analysis of worldwide Internet traffic data and characteristics, for Network Neutrality-related and other purposes, based on a distributed architecture of processes running mainly on end-user computers.

I've now dubbed this project the "Global Internet Measurement Analysis Array" (GIMAA).

I'd like to now touch very briefly on a few of the many practical considerations that such a project would entail, including deployment, security, and privacy issues.

To be useful, the measurement collection environment requires a very large number of participating end-user sites. While standalone

versions of the GIMAA programs will of course be needed for a variety of hardware platforms, deployment could be significantly hastened by including the associated code into other already widely used end-user packages, e.g. popular browser/OS toolbars and/or free utility application bundles. It may even prove possible to primarily use the existing application/toolbar data traffic as the foundational operational corpus for the measurement system itself, supplanted as necessary by purpose-generated measurement-related data.

To the extent that the vendors of such toolbar and application packages are interested in the potential ongoing output of a GIMAA environment, such "packaging" would seem an attractive possible route for dissemination of the system, with the goal of reaching a practical deployment level as quickly as possible.

A range of security and privacy issues accompany a project like GIMAA, some of which will likely be leveraged by some entities into objections against the entire project.

Clearly the GIMAA code modules, measurement payload data, and any associated aggregated data will need to be secure and as protected against manipulation and tampering as current technology will allow. User data on participating systems must be protected as a first priority concern.

A more unique issue with the GIMAA methodology is that the techniques envisioned, if they prove out and are very widely deployed,

could be extremely powerful. As such, concerns are sure to be raised that GIMAA may publicly reveal network traffic, topological, vulnerability, and other data that some network participants, and others, might prefer to keep hidden for business, security, or other reasons.

It can be anticipated, for example, that some firms (including ISPs) would become concerned that GIMAA node activity could reveal what they consider to be proprietary aspects of their network topologies, and that attempts to block GIMAA measurement traffic, and/or the writing of prohibitions against such measurement techniques into Terms of Service agreements, would be forthcoming.

Of course, one of the key purposes proposed for GIMAA is to detect vulnerabilities and abuses so that they can be corrected (through technical or policy means, as appropriate), and it would be expected that some of those entities responsible for such conditions would not be enthusiastic about their being so exposed.

I also consider it likely that GIMAA will be criticized from some quarters on national security grounds, with the argument being that the Internet infrastructural data that could be exposed would make attacks on the Internet and its attached systems more effective.

All of these concerns are real, and considerable effort will be needed to balance the benefits and risks associated with a project like GIMAA.

But aside from the more obvious cost/benefit analysis that can be applied to this project, there's another basic reality that renders some of these concerns relatively moot in important respects.

The categories of measurement methodologies proposed for GIMAA could be deployed on a clandestine basis by technologically skilled adversaries, perhaps as part of widely disseminated computer viruses and the like. If GIMAA does not move forward, that doesn't guarantee that "bad guys" won't get access to such data via their own GIMAA-like technologies that could infect systems around the world. Blocking GIMAA would only assure that honest players wouldn't have access to the same sorts of important information.

In my book, it's nonsensical and dangerous to block open and honest use of even potentially sensitive data, while the unscrupulous can likely gain access to similar data via their own means and for their own purposes. Sometimes sunlight really is the best disinfectant, and in the case of the Internet the old paradigm of "security through obscurity" has been widely discredited.

GIMAA, while not without real risks, will hopefully shed some needed light on aspects of the operational Internet that have been in the shadows for far too long, having caused a resulting lack of trust that only more open availability of data in these respects can likely ameliorate.

Thanks as always for your consideration.

Lauren Weinstein lauren@vortex.com or lauren@pfir.org +1 (818)
225-2800

Lauren's Blog: <http://lauren.vortex.com> PRIVACY Forum: <http://www.vortex.com>

✦ More Regarding the Online Medical Records Trap

<Lauren Weinstein <lauren@vortex.com>>

Fri, 05 Oct 2007 08:59:50 -0700

<http://lauren.vortex.com/archive/000307.html>

In response to my discussion of "The Online Medical Records Trap" (<http://lauren.vortex.com/archive/000306.html>), I've been asked what would happen if a central medical records system were encrypted in the manner I suggested, where the service provider couldn't access the records even in the face of an outside demand (like a court order) without the user's permission, in the case of the person being incapacitated or unconscious.

There are several rather simple answers to this. The most basic is that to depend on a centralized system as the only location where medical records are stored would be incredibly foolhardy. If doctors or hospitals needed access to that data, and their local computers or Internet connections were down, or if the central servers had been hacked or were having other

problems (including possible connectivity issues) then patients would be S.O.L. (that is, up the creek without a paddle).

It should be required that doctors and hospitals maintain local copies of patient records, ideally not only on their local computers (the same level of encryption and access control that I propose for central medical records systems would not be necessary nor desirable on these local systems), but also the records should be kept in hardcopy form as well.

Yes, I said hardcopy. A hassle that devalues the computerized systems?

Yep, but I want my medical records kept locally in a form that doesn't depend on computers or even electricity. I like those manila folders on the shelves, especially living in an area where earthquakes and other natural disasters (with their resulting power outages) are always a possibility. Most other areas also have their own risks of disasters or problems that could make computer-based access to patient records impossible just when they're needed most, especially if those records are centralized and communications are down.

As far as access to a central system is concerned, nothing says that a user couldn't provide friends, next-of-kin, etc. with their access key, or even have it noted on whatever emergency contact information that they hopefully carry routinely. I have a slip of paper in my wallet with a few contact names and numbers for emergency use, mainly in case some idiot wipes me out making a left turn in front of me when I'm riding, but the point

is that
while carrying around your passwords isn't a great idea in the
general case,
this is one specific situation where it could make sense.

I should add that it's also wise to include on your contact
sheet full
information about any allergies or other serious medical
conditions that
exist so that responders will know about them in emergencies.
To depend on
access to a centralized medical system for such info in these
situations
could be disastrous, even if none of the central data were
encrypted or
otherwise access controlled -- there's no guarantee that the
central system
would be reachable when you might need it most.

So what does this all boil down to? A centralized medical
records system
should never be depended upon for anything other than secondary
access to
medical data, if that. Doctors and hospitals must be required
to maintain
local copies of patient data since there is no guarantee that
central
systems will be accessible at any given time, particularly in
disaster or
other emergency situations.

To help prevent misuse of central medical records systems, all
personal
medical data on those central systems should only be accessible
with the
permission of the user or their designated contacts, and should
be encrypted
in a manner that makes other access impossible. Period.
Anything short of
this opens up enormous abuse potential.

Lauren Weinstein lauren@vortex.com or lauren@pfir.org +1 (818)
225-2800

Lauren's Blog: <http://lauren.vortex.com> PRIVACY Forum: <http://www.vortex.com>

[In subsequent discussion, Curt Sampson noticed the "beta" tag below the

HealthVault logo doesn't make him very confident about putting all of his

and his family's critical health information into the system. He also

noted a nasty problem with their feedback facility. Lauren noted a cert

inconsistency there. Curt replied "I think I can get some sense of how

well your site is run by clicking on 'feedback', which first gives me:

'Unable to verify the identity of feedback.live.com as a trusted site.'"

PGN]



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 86

Wednesday 17 October 2007

Contents

- [Lessons from June International Space Station crisis](#)
[James Oberg via Pat Flannery](#)
- [Tokyo Train System Ticketing System Failure](#)
[Stuart Woodward](#)
- [Dutch railway offers too-easy access to customer profiles](#)
[Leon Kuunders](#)
- [Austin-area toll equipment double-billed 50,000 times](#)
[Arthur Flatau](#)
- [Car Remote Control Cipher KeeLoq Is Broken](#)
[Steve Klein](#)
- [License plate scanners in police cars](#)
[Rob McCool](#)
- [Changed dates of NZ Daylight Saving; unsurprising consequences](#)
[Donald Mackie](#)
- [Medical error: Double mastectomy after 2nd opinion](#)
[Ken Knowlton](#)
- [Bypassing Internet censorship](#)
[Mike Radow](#)

- [Risks of writing a novel with your cell phone](#)
[PGN](#)
 - [Re: Another case of Deploy First, Test Later](#)
[Henry Baker](#)
 - [Re: Fake blogs](#)
[Dan Yurman](#)
 - [What do you do with unwanted voting machines?](#)
[David Lesher](#)
 - [Election Law online video lectures](#)
[Avi Rubin](#)
 - [Symposium on Usable Privacy and Security 2007 CFP](#)
[Simson Garfinkel](#)
 - [REVIEW: "The Complete April Fools' Day RFCs", Limoncelli/Salus](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Lessons from June International Space Station crisis (James Oberg)

<Pat Flannery <flanner@daktel.com>>

Tue, 16 Oct 2007 12:51:30 -0500

[Source: James Oberg, Space Station: Internal NASA Reports Explain Origins of June Computer Crisis; Faulty computer design and corrosion of leads on the ISS. This is a useful article on lessons that need to be learned, even though the crisis was resolved. Read the article. PGN]
<http://www.spectrum.ieee.org/print/5598>

⚡ Tokyo Train System Ticketing System Failure

<"Stuart Woodward" <stuart@stuartwoodward.com>>

Sun, 14 Oct 2007 22:10:38 +0900

I wondered why the station staff were directing the commuters through the gates without showing their tickets or passes on Friday. The reason is given here:

All of the automated gates were down due to programming fault in the system that reads the RFID cards commonly used by commuters.

If the guard wanted to see my train pass I would have had to open up the Java applet on my phone which handles the renewal of the pass. It's possible that it would also have failed due to the ongoing problem. Also if the phone's battery is dead there is no way to see details about the commuter pass, so the only sensible thing to do was to let everyone ride for free that morning.

<http://search.japantimes.co.jp/cgi-bin/nn20071013a4.html>

stuart@stuartwoodward.com jp mobile: 090-6166-7976 phone: jp 050-5534-5450

<http://www.stuartwoodward.com/map> IM: stuartcw on skype, yahoo, googletalk

[Stuart seems to support the MAX of five sentences for all e-mail:

<http://five.sentenc.es>

It would certainly not work for RISKS, even if we resorted to James

Joycean sentences. But it would certainly be a relief otherwise. PGN]

⚡ Dutch railway offers too-easy access to customer profiles

<Leon Kuunders <leon@kuunders.info>>

Thu, 04 Oct 2007 09:29:40 +0200

In order to keep customer satisfaction at the highest level possible, the Nederlandse Spoorwegen (dutch railway) have enabled several online profiling features for their subscription holders. Through this website customers can change their full personal details, look at their (payment) history, change bank account numbers, order new products, or ask for a refund.

The registration process for this website uses a failed authentication scheme. The "register me as a new customer" process works as "I have lost my password". For registration the only thing the customer has to do is enter it's customer number, name and e-mail address, after which a confirmation e-mail will be sent to the address given.

But there is no check if there has been a previous registration, and if so, if the e-mail addresses are the same. To make matters worse the customer number and name are clearly visible printed on letters, magazines and cards that the company sends to it's customers. Thousands of people every year lose their card, and with it the full credentials to their personal profile.

In a reaction the dutch railway representative said they thought it was "a good service to their customers" and "we have no reports of any incidents." How this service relates to the strict dutch privacy laws the representative

couldn't tell. In the meantime the registration process is offline and changed, so more details, like birthdate, are asked before access to a profile is granted.

Noothoven van Goorstraat 14, 2806 RA, GOUDA <http://leon.kuunders.info>

W: +31 641 164 995 P: +31 620 624 702

✶ Austin-area toll equipment double-billed 50,000 times

<Arthur Flatau <flataua@acm.org>>

Thu, 11 Oct 2007 09:44:41 -0500

An article in the 9 Oct 2007 issue of the *Austin American Statesman* reports on drivers getting double billed on the relatively new toll roads in the Austin area. (I believe none have been in use for more than a year.)

"The problem has occurred one of every 600 times a car passed one of the roads' tolling points. Agency officials say that they have made a number of equipment and software changes in the past few weeks to virtually eliminate the problem -- the frequency would now be more like one in every 2,000 toll transactions ..."

<http://www.statesman.com/search/content/news/stories/local/10/09/1009tollglitch.html>

I was going to insert a funny comment about virtually eliminating the problem, but I can not come up with one that is funnier than the original

wording above.

The problem has to do with the "antennae on the overhead gantries" picking up the toll tag more than once as it pass through. I do not understand how this would be hard to fix in software. If the same toll tag is picked up more than once in a span of say 30-60 seconds, this be labeled as an error of some kind (as it would be impossible to drive through in that span of time).

Car Remote Control Cipher KeeLoq Is Broken

<Steve Klein <steveklein@mac.com>>

Mon, 15 Oct 2007 08:55:27 -0400

(This press release is brief and direct, so rather than summarize I'll quote it in full. -- SK)

KeeLoq is a cipher used in several car anti-theft mechanisms distributed by Microchip Technology Inc. It may protect your car if you own a Chrysler, Daewoo, Fiat, General Motors, Honda, Toyota, Volvo, Volkswagen, or Jaguar. The cipher is included in the remote control device that opens and locks your car and that activates the anti-theft mechanism.

Each device has a unique key that takes 18 billion billion values. With 100 computers, it would take several decades to find such a key. Therefore KeeLoq was widely believed to be secure. In our research we have found a method to identify the key in less than a day. The attack

requires access
for about 1 hour to the remove control device (for example,
while it is
stored in your pocket). Once we have found the key, we can
deactivate [sic]
the alarm and drive away with your car. The attack has been
extensively
tested using software simulations.

This research is the joint work between 3 research groups: the
computer
science department of the Technion, Israel, the research group
COSIC of the
Katholieke Universiteit Leuven (Belgium) and the Hebrew
University, Israel.

<http://www.cs.technion.ac.il/news/2007/222/>

✶ License plate scanners in police cars

<Rob McCool <robm@robm.com>>

Sat, 13 Oct 2007 16:38:36 -0700 (PDT)

<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2007/10/13/MNJFSO1NM.DTL>

The *San Francisco Chronicle* just published an article about
license plate
scanners in police cars and traffic enforcement vehicles,
systems which can
scan "50 plates a second" and "do make mistakes". The system was
used to
apprehend an attempted child abduction suspect, and is used for
a variety of
parking enforcement measures related to increasing revenue.

The enthusiasm for the systems in this article is tangible, and
it contains
a modicum of privacy-related concerns. There is a small

discussion of the risks of thieves and others changing their behavior given that they know this system is in use, and claims that police officers tried to keep it secret for that reason. The opportunities for privacy violations as well as harassment are pretty easy to imagine, as are the unexpected side effects that its error rate may cause.

The article briefly mentions that such systems are common in London and in casinos, with little discussion of any problems that may have come up.

✂ Changed dates of NZ Daylight Saving; unsurprising consequences

<Donald Mackie <donald@iconz.co.nz>>
Fri, 5 Oct 2007 21:42:37 +1200

Earlier this year the New Zealand government decided to extend the period of daylight saving by three weeks.

[http://www.nzherald.co.nz/section/1/story.cfm?
c_id=1&objectid=10436995](http://www.nzherald.co.nz/section/1/story.cfm?c_id=1&objectid=10436995)

This involved bringing the spring clock change forward by a week. There was some concern in the IT community prior to the change about the ability of systems to respond to the change.

[http://www.nzherald.co.nz/section/story.cfm?
c_id=5&objectid=10465119](http://www.nzherald.co.nz/section/story.cfm?c_id=5&objectid=10465119)
<http://computerworld.co.nz/news.nsf/news/>

B7358C622F0F2D76CC25733A00056C73

<http://www.geekzone.co.nz/content.asp?contentid=7254>

<http://www.microsoft.com/nz/msdn/timezone/default.msp>

The clocks changed last Sunday. Unsurprisingly the fixes have been incomplete - though not entirely devastating. My own organisation uses Outlook and many of us have synchronised calendars on a mix of iMates, Blackberries and other phones (ie at least three downstream OSs).

Most appointments on desktops were, thanks to the work Microsoft did, correct after the clock change. I only had one which was an hour out - the person who set this up has been on leave for a few weeks and I suspect their desktop hasn't been turned on in that time - thus not getting any fixing updates.

The portable device calendars have been a different matter with most (but irritatingly not all) appointments at the wrong time. Efforts to fix the issue on individual portables seemed to add to the confusion. Events entered by the individual behaved differently to those made by someone else. The low point was a meeting yesterday that attendees came to at 1300, 1400 & 1500.

It is hoped that things will come back to normal next week, the clock change would previously have happened next Sunday, the 1st Sunday in October. We'll see.

Don Mackie, Auckland, New Zealand

⚡ **Medical error: Double mastectomy after 2nd opinion**

<KCKnowlton@aol.com>

Thu, 4 Oct 2007 09:56:06 EDT

A woman has had a double mastectomy, after seeking a second opinion confirming that she had cancer. She didn't -- the second diagnosing doctor relied on the same mislabeled tissue sample. (For readers of RISKS, there must be a subtle lesson or two in this.)

<http://wcbstv.com/topstories/breast.cancer.mastectomy.2.312736.html>

<http://www.msnbc.msn.com/id/21127917/>

⚡ **Bypassing Internet censorship**

<Mike Radow <mikeradow@yahoo.com>>

Mon, 15 Oct 2007 14:46:42 -0700 (PDT)

There is an implied *social risk* when technology is used to *block* access to the full range of Internet resources, i.e., ''censorship''.

Ron Deibert is a Professor of Political Science and Director of the Citizen Lab at the University of Toronto. He just published a paper on ''By-Passing Internet Censorship''...: Everyone's Guide to By-Passing Internet Censorship for Citizens Worldwide

http://deibert.citizenlab.org/Circ_guide.pdf

His BIO:: <http://deibert.citizenlab.org/blog/Info>

Some of techniques described in the text (or in the included URLs) were new to me. It is likely that many RISKS readers will find this paper interesting and informative, too.

⚡ Risks of writing a novel with your cell phone

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

Fri, 5 Oct 2007 5:25:54 PDT

<http://online.wsj.com/public/article/SB119074882854738970.html?mod=blog>

When Satomi Nakamura uses her cellphone, she has to be extra careful to take frequent breaks. That's because she isn't just chatting. The 22-year-old homemaker has recently finished writing a 200-page novel titled "To Love You Again" entirely on her tiny cellphone screen, using her right thumb to tap the keys and her pinkie to hold the phone steady. She got so carried away last month that she broke a blood vessel on her right little finger. ...

[Source: Yukari Iwatani Kane, Ring! Ring! Ring! In Japan, Novelists Find a New Medium; Budding Scribes Peck Their Tales on Cellphones; Ms. Nakamura's Hurt Pinkie, *Wall Street Journal*, 26 Sep 2007; thanks to Charles C. Mann]

⚡ Re: Another case of Deploy First, Test Later (Re: Huge, [RISKS-](#)

24.85)

<Henry Baker <hbaker1@pipeline.com>>

Tue, 16 Oct 2007 12:15:12 -0700

"A foolish consistency is the hobgoblin of little minds." Ralph Waldo Emerson

Whether intended or not, one consequence of the widespread implementation of IEEE-754 floating point arithmetic is that almost every computer now gets exactly the same answer, down to the last little bit. This "answer" may be far from the "correct" answer, but at least all of the computers will be consistent. In the "old" (pre-754) days, running the same Fortran program on several different computers could uncover potential sources of error. No longer.

(This generic phenomenon of foolish consistency even has a technical name: "informational cascade" -- if everyone agrees, then everyone must be correct. See http://en.wikipedia.org/wiki/Informational_cascade)

I realize that using multiple types of arithmetic to uncover bugs in floating point code may not be particularly efficient, but it sometimes works. IEEE-754 also provided for rounding modes that would allow for "range" arithmetic in order to achieve the same ends with much greater efficiency. Unfortunately, no one seems to implement or utilize those rounding modes anymore.

✦ Re: Fake blogs (Evron, [RISKS-24.83](#))

<"Dan Yurman" <djysrv@gmail.com>>

Mon, 15 Oct 2007 12:33:18 -0600

The problem of fake blogs is significant for me in two ways. I operate a blog on nuclear energy and nonproliferation topics. First, my content is being ripped off without attribution to attract ad clicks on other web sites and fake blogs. Aggregators of all kinds are taking blog content and using it to generate their own ad revenue. Good luck on that because in the past year I haven't made so much as lunch money from the ads on my blog served up by Google.

Second, and the more relevant issue for this list, is my content is being used on fake web sites to drive clicks on links in search engine results sending unsuspecting users to fake blogs and via redirect to websites with NSFW content and malware. The fake blogs often have redirects embedded in them so that the fake blogspot site is never really seen. The user is taken directly to the malicious website.

More than two-thirds of my blog visitors per month come in via unique search terms for one-time retrieval of archived material. People who search on the topics covered by my blog usually have industry or government expertise and know what they are looking for. It is pretty hard to confuse a search for a

pop tart singer with one for spent nuclear fuel.

I've seen that visitors don't get to my blog on the first try. It annoys them that a serious, work-related search has been diverted into a fake blog or website. There are additional problems for users who's employers have zero tolerance for hitting URLs with NSFW content.

This phenomenon is due to the fact that fake blog sites contain the same search terms as mine because they copied the original. Search engines deliver their results indiscriminately and do not always help users separate the fake blogs from the real ones.

For instance, a recent post on an planned environmental review by the Nuclear Regulatory Commission on uranium mining in Wyoming was picked up by another legitimate blog. My post and theirs both appeared subsequently in bogus blogs with redirects to NSFW content. I am not posting the fake blog URL here because it is unsafe.

I have a niche subject blog which isn't a big site, but with traffic approaching 5,000 visitors a month this is getting to be a problem.

I've assembled a few tips to avoid trouble, which may be obvious to readers, but here they are anyway. Fake blogs often have numbers in the web site name preceding 'blogspot.com'. Also, fake blogs tend to show up further down in the search results, due in part to a smaller number of links to them, but not always. Another way around is to search blogs on Technorati and check

the "authority" of a blog containing content of interest. The more links from other blogs with similar topics, the more likely it is legitimate, but that could change. Some search engines include a snippet from the content, and if the words are gibberish, that's a dead giveaway. Finally, search on the blog name itself and see how it shows up in search engine results and what kind of content is in the snippets.

I have no way as an individual to stop the current problem. I'm certainly open to ideas for constructive group action. Also, please feel free to share with me authentication measures you use before clicking on a blog link in a set of search results. If there are enough of them that are useful, I'll assemble a blog post on it based on your contributions, with or without attribution as you wish, and post a link to it in a future message to this list.

Dan Yurman djysrv@gmail.com, <http://djysrv.blogspot.com> 1-208-521-5726

⚡ What do you do with unwanted voting machines?

<David Leshner <wb8foz@panix.com>>
Sat, 13 Oct 2007 14:16:27 -0400 (EDT)

It used to be that everyone wanted a Florida voting machine. {...} But now that Florida is purging its precincts of 25,000 touch-screen voting machines

bought after the recount for up to \$5,000 each, hailed as the way of the future but deemed failures after five or six years, no one is biting. {...}

[Source: Abby Goodnough, Voting Machines Giving Florida New Headache, *The New York Times*, 13 Oct 2007]

<http://www.nytimes.com/2007/10/13/us/politics/13voting.html>

Pre-RISKS-able story [i.e: one any regular RISK reader could see was coming from \$10E6 away...]:

Florida is now stuck with \$millions of worthless DRE voting machines. Like too many used car and overpriced condo owners; they still owe money on them.

The risks are old ones:

1. If you throw enough money at a bad problem; you can make it a REALLY bad problem...that will need more money.
2. Legislators alas, never learned "primum non nocere" as MD's do.
3. Spending money first, then studying the problem & spec'ing the solution later; is almost always a bad idea. While the failures are more spectacular in building bridges than buying computing appliances; the results are often similar.

Election Law online video lectures

<Avi Rubin <rubin@jhu.edu>>

Thu, 11 Oct 2007 14:22:40 -0400

The Election Law Program, a joint venture of the College of William and Mary School of Law and the National Center for State Courts has put some course material in the form of online video lectures on election issues online:

<http://icmeducation.org/electionlaw/>

Here is a listing of the lectures available from their web site. The last 3 are lectures that I gave there.

Segment 1: Why Election Law Cases Are Different
Professor Richard Hasen

Segment 2: Pre-Election Issues: An Overview
Professor Richard Hasen

Procedural Concerns Related to Pre-Election Litigation
Professor Richard Hasen

Substantive Concerns Related to Pre-Election Litigation
Professor Richard Hasen

Segment 3: Election Day issues
Professor Ned Foley

Segment 4: Post-Election Issues
Professor Ned Foley

Segment 5: Electronic Voting: Global Election Systems
Professor Aviel Rubin

Why Electronic Voting is Different
Professor Aviel Rubin

Electronic Voting Technologies: Strengths and Weaknesses
Professor Aviel Rubin

Avi Rubin, JOHNS HOPKINS UNIVERSITY, Computer Science; Technical Director,
Information Security Institute 410-516-8177 <http://www.cs.jhu.>

edu/~rubin/

✦ Symposium on Usable Privacy and Security 2007 CFP

<Simson Garfinkel <simsong@acm.org>>

Sat, 13 Oct 2007 22:27:09 -0700

CALL FOR PAPERS -- SOUPS 2008 [Pruned for RISKS. PGN]
Symposium On Usable Privacy and Security
July 23-25, 2008
Carnegie Mellon University, Pittsburgh, PA USA
<http://cups.cs.cmu.edu/SOUPS/>

The 2008 Symposium on Usable Privacy and Security (SOUPS) will bring together an interdisciplinary group of researchers and practitioners in human computer interaction, security, and privacy. The program will feature technical papers, a poster session, panels and invited talks, discussion sessions, and in-depth sessions (workshops and tutorials). Detailed information about technical paper submissions appears below. For information about other submissions please see the SOUPS web site <http://cups.cs.cmu.edu/soups/2008/cfp.html>.

TECHNICAL PAPERS

We invite authors to submit original papers describing research or experience in all areas of usable privacy and security. Topics include, but are not limited to:

- * innovative security or privacy functionality and design,
- * new applications of existing models or technology,

- * field studies of security or privacy technology,
- * usability evaluations of security or privacy features or security testing of usability features, and
- * lessons learned from deploying and using usable privacy and security features.

Papers need to describe the purpose and goals of the work completed to date, cite related work, show how the work effectively integrates usability and security or privacy, and clearly indicate the innovative aspects of the work or lessons learned as well as the contribution of the work to the field. Submitted papers must not substantially overlap papers that have been published or that are simultaneously submitted to a journal or a conference with proceedings. Accepted papers will appear in the ACM Digital Library as part of the ACM International Conference Proceedings Series. The technical papers committee will select an accepted paper to receive the SOUPS 2008 best paper award.

Papers may be up to 12 pages in length including bibliography, appendices, and figures, using the SOUPS proceedings template on the SOUPS web site. All submissions must be in PDF format and should not be blinded. In addition, you must cut and paste an abstract of no more than 300 words onto the submission form.

Submit your paper using the electronic submissions page for the SOUPS 2008 conference (<http://cups.cs.cmu.edu/soups/2008/submit.html>). A successful submission will display a web page confirming it, and a confirmation email is sent to the corresponding author. Please make sure you

receive that
confirmation email when you submit, and follow the directions in
that email
if you require any follow up.

Technical paper submissions will close at midnight, US East
Coast time, the
evening of Friday, 29 Feb 2007.

General Chair: Lorrie Cranor, Carnegie Mellon University

Interactive and In-Depth Session Chairs:
Andrew Patrick, National Research Council Canada
Konstantin Beznosov, University of British Columbia

Posters Co-Chairs: Rob Miller, MIT and
Jaime Montemayor, The Johns Hopkins University Applied Physics
Laboratory

Technical Papers Co-chairs: Jason Hong, Carnegie Mellon
University and
Simson L. Garfinkel, Naval Postgraduate School

REVIEW: "The Complete April Fools' Day RFCs", Limoncelli/Salus

<Rob Slade <rMslade@shaw.ca>>
Mon, 15 Oct 2007 12:38:37 -0800

BKAFDRFC.RVW 20070814

"The Complete April Fools' Day RFCs", Thomas A. Limoncelli/Peter
H.

Salus, 2007, 978-1-57398-042-5

%A Thomas A. Limoncelli funnybook@rfc-humor.com

%A Peter H. Salus <http://www.rfc-humor.com> peter@usenix.org

%C P.O. Box 640218, San Jose, CA 95164-0218

%D 2007

%G 978-1-57398-042-5

%I Peer-to-Peer Communications, Inc.
%O U\$19.95 800-420-2677 fax: 408-435-0895 info@peer-to-peer.com
%O [http://www.amazon.com/exec/obidos/ASIN/1573980420/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/1573980420/robsladesinterne)
[http://www.amazon.co.uk/exec/obidos/ASIN/1573980420/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/1573980420/robsladesinte-21)
%O [http://www.amazon.ca/exec/obidos/ASIN/1573980420/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/1573980420/robsladesin03-20)
%O Audience a+ Tech 2 Writing 2 (see revfaq.htm for
explanation)
%P 390 p.
%T "The Complete April Fools' Day RFCs"

For those in the know, the designation "RFC" is a bit of a joke in itself.

As a "Request For Comment," there is an implication of a proposal, as opposed to a standard. In fact, the RFCs are the "official" documents of the Internet protocols, and are part of a formal process. Given the nature of the Internet, and the people involved, it should come as no surprise that embedded in this library are jokes, making fun of the process as much as anything else.

(Just to make things clear, this is far from a compendium of all of the jokes flying around the net, or even all of the jokes about network standards. The April Fools' RFCs are a specific class of net jokes, and are the material of this volume.)

The RFCs themselves present a kind of technical history of the Internet. In a similar way, the April Fools' RFCs are a history of aspects of the Internet. Some of them document technical concerns and emphasis, such as the 1990s attempts to implement the Internet on any base

physical transport
(RFC 1149, dealing with avian carriers) or 2002's efforts to run
all
utilities over the Internet (RFC 3251, for providing electricity
over
Internet Protocol). Others reflect more general social concerns.

The RFCs are all freely available. This book collects all the
April Fools'
documents, and the authors have even made the collection
available on the
Internet. However, the print version contains additional
commentary,
structure, and supplementary background information about the
RFC authors.

And it's handy to have the dead trees edition for those times
when the avian
carriers aren't flying to your particular hotspot.

copyright Robert M. Slade, 2007 BKAHDRFC.RVW 20070814
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>

[Steve Bellovin's Evil Bit (and Drew Dean's Angelic Bit), both
of which

appeared in [RISKS-22.66](#) are both worthy, although only the
first one was a

"real" RFC. The "IP over Avian Carriers" is a real classic.
The material

is highly recommended for humor-loving RISKS readers.

Limoncelli and

Salus deserve many thanks for making this material so easily
accessible.

Of course many other non-RFC April Fools' spoofs are also
worthy, such as

Chernenko@MOSKVAX (Piet Beertema, 1 April 1984, pre-RISKS, but
reproduced

in my book, Computer-Related Risks, pp. 146-148) and the
April Fools'

warning message attributed to Gene Spafford ([RISKS-6.52](#)) come
immediately

to mind, even though the day of reckoning is still half a year away.

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

Search RISKS using [swish-e](#)

Volume 24: Issue 87

Monday 22 October 2007

Contents

- [Tix-Nix Rocks Rox-Sox Jox](#)
- [Computerised anti-aircraft gun kills 9](#)
[Gary Hinson](#)
- [Russian spacecraft lands short: "computer glitch"](#)
[Ken Knowlton](#)
- [Loss of control and crash of UAV](#)
[Ian Staines](#)
- [Re: LI Railroad double bills for tickets](#)
[Al Stangenberger](#) [Erik Mooney](#)
- [Re: Dutch railway offers easy access to customer profiles](#)
[Leon Kuunders](#)
- [Risks of cute e-mail](#)
[Chris Williams](#)
- [SSP 2008: Paper Submission Deadline: Friday, November 9, 2007](#)
[Yong Guan](#)
- [REVIEW: "Exploiting Online Games", Greg Hoggund/Gary McGraw](#)
[Rob Slade](#)
- [Info on RISKS \(comp.risks\)](#)

Tix-Nix Rocks Rox-Sox Jox

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

Mon, 22 Oct 2007 16:23:04 PDT

Mark Johnson contributed this item from the Colorado Rockies' website:

http://colorado.rockies.mlb.com/content/printer_friendly/col/y2007/m10/d22/c2276226.jsp

Sales of World Series tickets in Denver had to be suspended after "too much activity" on the servers. Fewer than 500 tickets were sold out of over 50,000. The current plan is to fix the online system and try again.

Mark also added:

Even more interesting is a *Denver Post* opinion piece that indicates over

200 clients lost the ability to sell tickets due to this server failure.

Nothing like putting all your eggs into one basket.

Joe Loughry added this gem from *The Denver Post*:

http://www.denverpost.com/ci_7248448

But some people found glitches, such as being told to "enable cookies" and

to set their computer security to the "lowest level." And some fans

couldn't log in at all.

Alves explained that those who saw a "page cannot be displayed" message

had "IP addresses that we blocked due to suspicious/malicious activity to

our website during the last 24 to 48 hours. As an example, if several

inquiries came from a single IP address they were blocked."

With baseball's so-called World Series between the Rockies and the Red Sox about to start on 24 Oct, this item seems timely. Maybe simultaneous overly large orders from scalpers brought down the server? All games will be broadcast on Fox, but will there be anyone in the stands?

With Rocks in their Socks,
And their Jocks on Fox,
The Rox in the Box
May get some Knocks
Off the Sox --
If they can DeTox,
Fix the Tix-Nix Mix-
up, and get in some Lix.
Rox or Sox in six?
Seven is heaven.

PGN

✶ Computerised anti-aircraft gun kills 9

<"Gary Hinson" <Gary@isect.com>>
Sat, 20 Oct 2007 11:29:38 +1300

[http://www.mg.co.za/articlePage.aspx?articleid=322117&area=/
breaking_news/br
eaking_news__national/](http://www.mg.co.za/articlePage.aspx?articleid=322117&area=/breaking_news/breaking_news__national/)

The story speaks for itself. After the operators cleared a jam in a Swiss/German Oerlikon 35mm Mark V anti-aircraft twin-barreled gun during a live-firing military exercise [at the South African National Defence Force

Lohatlha training grounds], the gun turned to the left and fired a rapid burst of cannon shells directly at adjacent guns in the line, killing 9 soldiers and injuring 14. At the time, the gun was supposedly on 'manual', locked on to a target 1.5 to 2km away. On 'manual', it should not have turned at all.

<http://www.itweb.co.za/sections/business/2007/0710161034.asp?S=IT%20in%20Defence&A=DFN&O=FPTOP>,

According to "Defence pundit Helmoed-Roemer Heitman told the Weekend Argus that if 'the cause lay in computer error, the reason for the tragedy might never be found.'" If 'computer error' equates to bug, then I can only assume the software must be horrendously complex and opaque to be so resistant to analysis ... which it probably is if it combines target acquisition/identification, range finding, gun control, oh and safety.

The South African Department of Defence is under pressure to conduct an inquiry.

[http://www.mg.co.za/articlePage.aspx?articleid=321877&area=/breaking news/breaking news national/](http://www.mg.co.za/articlePage.aspx?articleid=321877&area=/breaking%20news/breaking%20news%20national/)

Don't the procurers of such automated weaponry specify mechanical safety interlocks capable of physically preventing the turret from turning beyond set azimuth (and perhaps elevation) limits?

[Other reports on this noted by Ilya Gulko, Martin Ward, and Kurtis Lanovaz. PGN]

✈ **Russian spacecraft lands short: "computer glitch"**

<Ken Knowlton <KCKnowlton@aol.com>>

Sun, 21 Oct 2007 13:21:39 EDT

A Russian spacecraft came down a minute early, on a steeper-than-planned descent, and landed 210 miles off from its designated site, due to a "computer glitch." And nobody got hurt. Said Alexei Krasnov, head of the Russian space agency's manned space programs, "It's difficult to immediately name a specific reason behind the problem. We need to do an in-depth analysis." (AP 21 Oct 2007)

<http://www.abcnews.go.com/Technology/wireStory?id=3756743>

✈ **Loss of control and crash of UAV**

<"Staines, Ian" <istaines@rsasecurity.com>>

Fri, 19 Oct 2007 19:50:07 -0400

AVweb has a good article on the recent loss of control and crash of an UAV (Unmanned Arial Vehicle).

http://www.avweb.com/avwebflash/news/NTSB_CustomsBorderPatrol_UAVcrash_196405-1.html

The full article is an even better read. See the full NTSB report:

http://www.nts.gov/nts/brief2.asp?ev_id=20060509X00531&ntsbno=CHI06MA121&akey=1

There are numerous automation and user faults that RISKS readers

will find
familiar.

I think what is poignant here is that although these vehicles have a fairly long history of use within the military these aircraft are now being integrated into the civilian airspace. They are also flying along international borders and potentially in international airspace. Especially troubling for me is this quote: "...Because of national security issues and past experience with similar UASs, the FAA temporarily waived this requirement for the issuance of the Certificate of Waiver or Authorization (COA) to operate in the National Airspace System (NAS)..."

Ian Staines, Delta, BC, CANADA, istaines@shaw.ca

⚡ Re: LI Railroad double bills for tickets ([RISKS-24.86](#))

<Al Stangenberger <forags@nature.berkeley.edu>>
Sat, 13 Oct 2007 21:50:20 -0700

The railroad now says that the problem was caused by a software update in late September, rather than an error undiscovered since 2001. They have reverted to the previous version of the software and are revising their testing procedures.

<http://www.newsday.com/news/local/wire/newyork/ny-bc-ny--lirrdoublebilling1011oct11,0,3782883.story>

✶ Re: LI Railroad double-bills for tickets ([RISKS-24.86](#))

<Erik Mooney <erik@dos486.com>>

Thu, 11 Oct 2007 16:39:41 -0500

Anybody want to bet that the problematic limit was precisely 32,767? :)

This glitch actually hit me personally - I had a LIRR ticket double-billed.

I didn't bother with LIRR customer service, since I had no evidence to

convince a commuter railroad that I didn't ride it two days in succession.

I was waiting for the credit card statement to cycle so I could dispute it

at that level, but fortunately the merchant (the railroad) discovered its

error and credited the account. 'Twas strange, after reading RISKS for

years to find myself actually caught in one!

[R.G. Newbury and Scott Nicol also suggested this likely explanation.

Scott: "Could this have been a 16-bit signed int rollover bug?" PGN]

✶ Re: Dutch railway offers easy access to customer profiles ([R-24.86](#))

<Leon Kuunders <leon@kuunders.info>>

Fri, 12 Oct 2007 00:24:21 +0200

For what it's worth: in the meantime some minor inconsistencies (spelling

errors, very broad error messages that include instructions on

how their cards are numbered) have been detected on their website. Also, and of more interest, is the way their privacy policy is set up: they point for part of the transaction process to another company (owned by 5 large Dutch public transport organizations), who in return point back at them. Bottom-line: they can (and will) identify you, even if you are using an anonymous card, through the bank-transaction that is needed to buy the (anonymous) card...

Noothoven van Goorstraat 14, 2806 RA, GOUDA <http://leon.kuunders.info>

W: +31 641 164 995 P: +31 620 624 702

⚡ Risks of cute e-mail

<Chris Williams <cwilliams@jabber.com>>

Thu, 11 Oct 2007 11:40:18 -0600

Recently here in the Denver area, a very cute e-mail has been making the rounds. The story goes:

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

Scott rescued 6 black lab (mix) puppies out of the middle of the road on

Saturday. PLEASE help me find them homes - otherwise, it's Animal Control

- which means they only have 5 days. We've bathed them, sprayed them for

fleas and wormed them....but we can't keep them. They are currently in a

kennel in my basement since I don't have a fence. I've lost

count of the

number of rescue groups that I've contacted, only to be turned down due to no room.

Please check with every dog person you know to see if they need a puppy.

Regards,

Tim Aumack

If you know someone looking for a pet, please contact:
Bryan Pratt , CPA, Manager - Corporate Tax, Bill Barrett Corporation

.... 18th Street, Suite 2300, Denver , CO 80202 PH: 303-293-....

FAX: 303-291-.... DIR: 303-312-.... bpratt@<domainname deleted>

-----End Message-----

And of course there was a appropriately cute picture attached of six black lab mix puppies (omitted here).

I first saw this e-mail early last week as it made the rounds at my girlfriend's place of work. A day or so later I heard from several other friends and they forwarded it along as well. Now this week it appears to still be circulating as it made it to my work as well. It does appear that this is (or was originally) a legit e-mail and the photo attached was just that, but the RISKS here are several:

1) Who needs a bot army to send spam/viruses when you can get people to willingly forward things along for you?

2) If you attach a picture with something as cute as puppies looking for a

home, everybody is going to open it.

3) Since this appears to have started as a local phenomenon and has slipped

by every anti-spam and anti-virus engine, the potential for malice is

high.

4) Before speculating on the legitimacy of something in a public forum,

research, research, research!

A search of the interwebs revealed this e-mail to be a nationwide phenomenon.

Despite the fact this e-mail is indeed a hoax, it doesn't detract from the validity of the first three RISKS.

It will be interesting to see if this e-mail makes it out of the Denver/Boulder area to other parts of the country or if we see someone on

the dark side take this localized phenomenon and twist it to work for the dark side.

chris williams, manager of information technology, jabber, inc.
1-303.308.3292

[Address, phone numbers & e-mail address in the original e-mail suppressed.-c]

SSP 2008: Paper Submission Deadline: Friday, November 9, 2007

<Yong Guan <guan@iastate.edu>>

Tue, 16 Oct 2007 20:15:27 -0500

2008 IEEE Symposium on Security and Privacy

The Claremont Resort, Berkeley/Oakland, California, USA, May 18-22, 2008

PAPER SUBMISSION DEADLINE: Friday, 9 Nov 2007 23:59:00 EST (GMT-5)

(No extensions!)

For more information on the symposium, please visit:

<http://www.ieee-security.org/TC/SP2008/oakland08.html>

REVIEW: "Exploiting Online Games", Greg Hoglund/Gary McGraw

<Rob Slade <rmslade@shaw.ca>>

Mon, 22 Oct 2007 10:16:10 -0800

BKEXONGA.RVW 20070913

"Exploiting Online Games", Greg Hoglund/Gary McGraw, 2008,
0-13-227191-5, U\$44.99/C\$55.99

%A Greg Hoglund www.rootkit.com

%A Gary McGraw www.exploitingonlinegames.com gem@digital.com

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8

%D 2008

%G 978-0-13-227191-2 0-13-227191-5

%I Addison-Wesley Publishing Co.

%O U\$44.99/C\$55.99 416-447-5101 fax: 416-443-0948 bkexpress@aw.com

%O [http://www.amazon.com/exec/obidos/ASIN/0132271915/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0132271915/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/0132271915/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0132271915/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/0132271915/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0132271915/robsladesin03-20)

%O Audience i+ Tech 2 Writing 2 (see [revfaq.htm](#) for
explanation)

%P 340 p.

%T "Exploiting Online Games: Cheating Massively Distributed
Systems"

Shall We Play A Game? or

Being a Review of "Exploiting Online Games"

With Much Editorializing and Extensive Digressions

Fair warning, then: this review is going to be a bit different.

Why games? Isn't this topic a bit trivial? After all, Hoglund and McGraw are among the very select few who have been able to use the "hack to protect" style work. By examining vulnerabilities they have created books like "Software Security" (cf. BKSWSBSI.RVW) that have contributed useful guidance to those attempting to build more robust and reliable programs. Therefore, the foreword, preface, and first chapter all attempt to provide reasons why such a book is needed.

First off, there is a very large virtual economy that interpenetrates with the [real|cash] one. Since gamers have started selling abilities, "game gold," and even characters, game objects now have cash values in the real world. As with anything that has an exchangeable value, the criminal world has taken an interest. Trade in game objects now comprises a large fraction of online frauds, identity theft, and money laundering. (The trojan posted at the Dolphin Stadium Website, and others, around SuperBowl time had a subordinate payload looking specifically for "World of Warcraft" accounts.)

Everything that relates to software insecurity (and security) in the online gaming environment applies (though possibly not equally) to security in other systems. Therefore, a book noting the security vulnerabilities of game systems provides an introduction to system security in general, and

application security in particular. It helps that the gaming topic is of intrinsic interest to a number of people, and therefore may spark interest in information security.

(Interestingly, no argument is made in the book is that the existence of vulnerabilities in the game system itself, and particularly on the client side, may open the gamer to various forms of attack [and not just by axe-swinging berserkers]. Loopholes in the client software could lead to openings for intrusions, means of gaining information about the user or system, or entry points for malware. We have seen numerous instances of problems associated with widely used client software packages, such as those for instant messaging and peer-to-peer file sharing.)

Chapter two contains a discussion of various ways of manipulating games. Most of these are at a conceptual level, although some are extremely detailed, including macro and C code. The material also addresses some countermeasures to the cheats, and a few ways to defeat the safeguards, as well. Instances and examinations of the virtual economies that have sprung up around online games are presented in chapter three. Given the earlier stress on the importance of the point (as a rationale for the book itself), the content is disappointingly thin in this separate chapter. American copyright and related laws (particularly the Digital Millennium Copyright Act) and End-User Licence Agreements are the substance of chapter four.

Chapter five notes a number of bugs, primarily those involving interactions of complex functions and states of games. Tools and techniques for examining and manipulating client software are described in chapter six. There is a lot of C code, and, although the programming is extensive it can't be exhaustive, since the chapter basically covers a topic to which whole books are devoted. (Most of the suggestions are directed at attacking the server, and, again, there are few mentions of the risks of vulnerabilities in the client.) Chapter seven provides C code for programming robots to cheat at the game for you. The chapter seems oddly placed, since eight returns to the topic of reverse engineering of software, and lists more tools. (There is also a rather comprehensive guide to basic functions in assembly code.) Advanced game hacking, in chapter nine, deals mostly with the modification of clients or the creation of alternate game servers.

Chapter ten starts off with the statement that the primary goal (of the book) is to "understand the security implication of massively distributed software systems that have millions of users." That's a worthy goal, and one that is indicated by the subtitle. Therefore, it is strange to note that not only is this intent omitted from the rationale given at the beginning, but also that the topic really isn't addressed in the text. There are so many notions that could be explored under that subject, such as the social engineering aspects of working with large groups, the emergent

properties that might arise from simple functions operating in large numbers of nodes, the massive power of distributed systems, or even the relation to the botnets that are currently such a concern. None of these ideas are explored in the book or in chapter ten itself, which is simply a fairly brief review of some decent but basic software security guidelines.

The book is, therefore, a partial success. The introduction to the fundamentals of software security via the gaming medium is a potentially useful and valuable device. The work does tend to concentrate more on the game aspects, and less on the generic principles, but that emphasis is not necessarily a flaw. The precepts are sound, and those who do become interested in security will be able to apply them, and move on to more advanced areas.

copyright Robert M. Slade, 2007 BKEXONGA.RVW 20070913
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<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

Search RISKS using [swish-e](#)

Volume 24: Issue 88

Weds 31 October 2007

Contents

- [Rox-Shocks Tix-Nix Fix](#)
[PGN](#)
- [Normal hardware upgrades may deactivate Microsoft Vista\(tm\)](#)
[Mike Radow](#)
- [German Telephone-Network Partial Outage](#)
[Peter B. Ladkin](#)
- [A computer-related fatality](#)
[Martyn Thomas](#)
- [Anti-DWI interlocks considered for ALL drivers](#)
[D.F. Manno](#)
- [Risk of laptop computer on a commercial aircraft](#)
[jared](#)
- [LoJack undoes scheme to fake SUV theft](#)
[Paul Saffo](#)
- [Trojan Horse Redirects Local DNS Settings to Malicious DNS Servers](#)
[Monty Solomon](#)
- [Think before you legislate](#)
[Robert S. Heuman](#)

- [Court filing in TJX breach: 94 million accounts affected](#)
[Monty Solomon](#)
 - [Restaurant chain customers' credit card data stolen](#)
[Monty Solomon](#)
 - [Fighting traffic citations](#)
[Steve Greenwald and Jeremy Epstein via PGN](#)
 - [Gatwick Airport screens display wrong local time](#)
[Philippe Jumelle](#)
 - [TV PVRs getting BST change not quite right](#)
[Nick Rothwell](#)
 - [DST traffic signal snafu](#)
[D. Joseph Creighton](#)
 - [Who set up that meeting anyway?](#)
[Jeremy Epstein](#)
 - [US Congress pulls the classic e-mail oopsie](#)
[Danny Burstein](#)
 - [Who needs bots?](#)
[Matt Simpson](#)
 - [Re: Fake blogs](#)
[Dan Jacobson](#)
 - [Same ol' same ol'](#)
[Andrew Koenig](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Rox-Shocks Tix-Nix Fix (Re: [RISKS-24.87](#))**

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

Wed, 31 Oct 2007 15:12:09 PDT

After last Monday's (22 Oct 2007) presumed denial-of-service attack that hindered Denver's World Series ticket sales, reportedly with over 8 million bogus hits on the website, Tuesday's efforts were much more successful. The

Rockies sold out every ticket for games 3, 4, and 5 [which, as it turns out, was not needed] in about 2.5 hours. That's a total number of tickets three times the seating capacity of 50,445, which works out to an average of just about 1000 tickets per minute. It would take a large cadres of human ticket sellers to keep up that rate. Thus, automation of this kind clearly has its merits -- when it works securely and reliably (modulo some presumed amount of credit-card fraud). However, blocking multiple requests from the same IP address seems to be overly aggressive -- for example, for groups of would-be buyers behind firewalls, although it might have slowed down the scalpers. [Actually, the Rockies suffered a much more costly denial-of-service attack at the hands (and feet) of the Red Sox.]

⚡ Normal hardware upgrades may deactivate Microsoft Vista(tm)

<Mike Radow <mikeradow@yahoo.com>>
Tue, 23 Oct 2007 17:14:35 -0700 (PDT)

Microsoft attempts to determine when your **registered** copy of their Operating System has been moved to another computer.

The concept is simple...: Different hardware components are identified during the registration process and a **weighted** hash is computed from model numbers, MAC addresses, etc. This can -- supposedly -- differentiate innocent user-upgrades from proscribed outright copying. At least, that is

their claim and the heuristic's intent.

When it comes to monitoring Microsoft Vista(tm), this process may not be

perfect. Perhaps it is a bit too touchy in the 'False Positive'

department. At least this is what Slashdot reports, at...:

<http://slashdot.org/article.pl?sid=07/10/23/1255235>.

As reported in the 23.X.2007 issue of the Australian Consolidated Press

(ACP) magazine, '... something as small as swapping the video card or

updating a device driver can trigger a total Vista deactivation.'

The full ACP story is at http://apcmag.com/vista_activation , , ,

This article seems to identify a major hazard (read 'show-stopper') to

everyday regular maintenance!

🔥 German Telephone-Network Partial Outage

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>

Wed, 31 Oct 2007 09:10:32 +0100

On 29 Oct 2007 a software update to a billing server in the network of the

former Deutsche Telekom (German Telecom) in Düsseldorf resulted in many

telephone numbers nationwide becoming unreachable. The outage lasted between

about 4pm and 9pm. Apparently it also affected some portions of the mobile

telephone network. (It affected me also, but one of my numbers carried on

working. I contract with another service provider.)

Deutsche Telekom is the privatised former state telephone network and still the majority infrastructure owner in Germany, which is why the outage affected those such as myself who do not contract for service with DT. It affected people all over Germany, but DT doesn't say how many.

SW updates are a "daily occurrence" according to a spokesman. They went back to a previous version and they are inspecting the problem SW now to see what caused the outage.

(Personal experience, aided by reports in the Neue Westfälische Zeitung, 30 and 31 Oct 2007)

Peter B. Ladkin, Causalis Limited and University of Bielefeld
www.causalis.com www.rvs.uni-bielefeld.de

⚡ A computer-related fatality

<Martyn Thomas <martyn@thomas-associates.co.uk>>
Sat, 27 Oct 2007 10:54:11 +0100

A Texas judge, Sharon Keller, refused to keep her court open for 20 minutes to receive an appeal from the lawyers representing Michael Richard. He was executed later the same night.

His lawyers had suffered a computer breakdown and said they were unable to file the appeal within regular working hours. They had begged Judge Keller for more time and she refused.

Her decision might have gone unnoticed had the supreme court not announced, on September 25, that it was reviewing a challenge to the legality of lethal injection.

The announcement set off a flurry of appeals from death-row inmates and it is believed Richard's execution most likely would have been halted, to await the supreme court decision, had he been granted a hearing. Two days after Richard was executed, the supreme court blocked a lethal injection in Texas. Judges in Alabama and Kentucky have also stayed executions, bringing in an unofficial moratorium on the death penalty.

<http://www.guardian.co.uk/usa/story/0,,2199596,00.html>

⚡ Anti-DWI interlocks considered for ALL drivers

<"D.F. Manno" <dommanno@yahoo.com>>

Wed, 24 Oct 2007 14:25:08 -0700 (PDT)

The New York Times (21 Oct 2007), in a article that may not have been widely noticed because it was buried in the Automotive section, reports that automakers and researchers, with U.S. government funding, are working on anti-drunk-driving interlocks that ALL drivers will have to pass in order to drive their cars, whether or not they have a record for DWI.

<<http://www.nytimes.com/2007/10/21/automobiles/21ALKY.html>>

Among other things, the article notes that to start a car with

the interlocks currently used, ``the driver must puff a breath into the unit. To avoid cheating, the breath puff is measured and must be given in a uniquely identifiable way that would be hard for a person who is not the driver to duplicate.'' The breath puff isn't just for starting cars. While driving, the driver must periodically blow into the system to keep the car running."

The researchers acknowledge that the current technology is not reliable or durable enough to install in all cars. But the capabilities to determine who is taking the test and to require periodic retesting while driving would presumably be carried over into the newer systems.

Aside for the Big Brother and Prohibition aspects, to me the RISK with both current and future systems seems to be that your car can automatically stop -- regardless of road, weather or traffic conditions -- if you don't have time or can't split your attention to take the test (while doing 65 mph on the freeway, or while you're dealing with your children in the back seat), or if there's a false positive, or if the equipment is faulty.

✦ Risk of laptop computer on a commercial aircraft

<jared <jared@netspace.net.au>>
Sun, 28 Oct 2007 08:43:23 +0000

"Jet forced to land by a runaway laptop" is a headline in the 26 Oct 2007

Jewish Chronicle (www.thejc.com). In summary, a London-Tel Aviv flight made an unscheduled stop at Athens. A laptop has been found on-board which no one nearby claimed. Per security procedures the plane made an impromptu landing. At which point the computer's owner, having woken up, asked if anyone had seen a missing laptop.

LoJack undoes scheme to fake SUV theft

<Paul Saffo <psaffo@mac.com>>
Wed, 31 Oct 2007 10:19:10 -0700

Talk about dumb and dumber...

[Source: San Diego *Union-Tribune*, 31 Oct 2007; PGN-ed]
<http://www.signonsandiego.com/news/northcounty/20071031-0755-bn31car.html>

Sheriff's officials say an Oceanside [CA] woman who was behind on car payments faked that her 1999 GMC Yukon was stolen and hid it in a friend's backyard in Escondido, not realizing it was equipped with a LoJack system. After she filed a stolen vehicle report and an insurance claim, police activated LoJack and found the SUV in a friend's yard with the woman's boyfriend's old plates.

["'Lo, Jack? How's Jill?" "She's 'Jilling." PGN]

🔴 Trojan Horse Redirects Local DNS Settings to Malicious DNS Servers

<Monty Solomon <monty@roscom.com>>

Wed, 31 Oct 2007 16:18:37 -0400

INTEGO SECURITY ALERT - October 31, 2007

OSX.RSPlug.A Trojan Horse Changes Local DNS Settings to Redirect to Malicious DNS Servers

Exploit: OSX.RSPlug.A Trojan Horse

Discovered: October 30, 2007

Risk: Critical

Description: A malicious Trojan Horse has been found on several pornography web sites, claiming to install a video codec necessary to view free pornographic videos on Macs. A great deal of spam has been posted to many Mac forums, in an attempt to lead users to these sites. When the users arrive on one of the web sites, they see still photos from reputed porn videos, and if they click on the stills, thinking they can view the videos, they arrive on a web page that says the following:

Quicktime Player is unable to play movie file.
Please click here to download new version of codec.

After the page loads, a disk image (.dmg) file automatically downloads to the user's Mac. If the user has checked Open "Safe" Files After Downloading in Safari's General preferences (or similar settings in other browsers), the disk image will mount, and the installer package it contains will launch Installer. If not, and the user wishes to install this codec,

they

double-click the disk image to mount it, then double-click the package file, named install.pkg.

If the user then proceeds with installation, the Trojan horse installs; installation requires an administrator's password, which grants the Trojan horse full root privileges. No video codec is installed, and if the user returns to the web site, they will simply come to the same page and receive a new download.

<http://www.intego.com/news/ism0705.asp>

Think before you legislate

<RsH <robert.heuman@alumni.monmouth.edu>>

Tue, 23 Oct 2007 22:20:28 -0400

Elections Act changes deny vote for 1 million Canadians, CBC News 23 Oct 2007

The federal government said Tuesday it will fix a problem with the newly revamped Elections Act that prevents up to a million rural voters from casting a ballot.

Four months ago, Parliament passed amendments to the Canada Elections Act that requires each voter produce proof of identity and a residential address before being allowed to cast a ballot.

However, more than one million Canadians living in rural areas don't have an

address that includes a street name and number.

Rural addresses are often just post office boxes. On native reserves, a resident's address is sometimes simply the name of the reserve.

In Nunavut, more than 80 per cent of registered voters don't have a residential address.

Government House Leader Peter Van Loan told Parliament Tuesday that the problem was an oversight and called on all parties to "enthusiastically support efforts to correct this deficiency."

Van Loan also said if a snap election were to be called before the issue is resolved, the chief electoral officer has assured him that he's prepared to use "his adaptation power to ensure that no Canadian loses their right to vote" in the ensuing election.

With files from the Canadian Press

R. S. (Bob) Heuman <robert.heuman@alumni.monmouth.edu>

🔥 Court filing in TJX breach: 94 million accounts affected

<Monty Solomon <monty@roscom.com>>

Thu, 25 Oct 2007 02:04:37 -0400

More than 94 million accounts were affected in the theft of personal data from TJX Cos., a banking group alleged in court filings, more than twice as many accounts as the Framingham retailer has said were affected in what was

already the largest data breach in history. The data breach affected about 65 million Visa account numbers and about 29 million MasterCard numbers, according to the court filing, which was made late yesterday by a group of banks suing TJX over the costs associated with the breach. The banks cited sealed testimony taken from officials at the two largest credit card networks. A Visa official also put fraud losses to banks and other institutions that issued the cards at between \$68 million and \$83 million on Visa accounts alone, the filing states, the most specific estimate of losses to date.

TJX, which operates more than 2,500 stores worldwide under such brand names as TJ Maxx and Marshalls, previously has said the unidentified hackers who breached its systems had compromised at least 45.7 million credit and debit card numbers as far back as 2003. TJX has said about 75 percent of the compromised cards were expired or had data in the magnetic strip masked, meaning the information was stored as asterisks rather than numbers. ...

[Source: Ross Kerber, Court filing in TJX breach doubles toll: 94 million accounts were affected, banks say, *The Boston Globe*, 24 Oct 2007]

http://www.boston.com/business/globe/articles/2007/10/24/court_filing_in_tjx_breach_doubles_toll/

Restaurant chain customers' credit card data stolen

<Monty Solomon <monty@roscom.com>>

Thu, 25 Oct 2007 01:59:51 -0400

Not Your Average Joe's, a Massachusetts restaurant chain, said yesterday that thieves have stolen credit card data belonging to its customers. The Dartmouth-based chain estimated fewer than 3,500 of the 350,000 customers it served in August and September had their credit card information stolen.

The 14-restaurant chain said it is working with the US Secret Service and major credit card companies to determine how the data theft occurred and precisely how many customers were affected. [Source: Bruce Mohl, *The Boston Globe, 24 Oct 2007]

http://www.boston.com/business/globe/articles/2007/10/24/restaurant_chain_customers_credit_card_data_stolen/

[Small potatoes, you say? But the customers were fried, and now they're playing catchup. PGN]

⚡ Fighting traffic citations

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

Fri, 26 Oct 2007 11:51:38 PDT

In an out-of-band communication, Steven J. Greenwald (sjg6@gate.net) pointed out an AP item by Lisa Leff, Teen's ticket hinges on GPS vs. radar, 25 Oct

2007, in which a retired sheriff's deputy had used a GPS tracking device to keep an eye on his stepson Shaun's driving habits. This annoyed

Shaun -- at least until he was pulled over for allegedly doing 62 in a 45-mile-per-hour zone. The GPS unit showed that he was indeed doing the speed limit.

Whether this is sufficient evidence is still pending.

http://news.yahoo.com/s/ap/20071025/ap_on_hi_te/gps_ticket_challenge_2&printer=1; ylt=AnZr6gtZnk0ZUsM9p9w..vVk24cA

This item reminded Jeremy Epstein <Jeremy.Epstein@SOFTWAREAG.COM> of a case over 30 years ago where a physicist at Los Alamos Labs protested a speeding ticket by trying to convince the judge (who was a retired physicist from the labs) that the thunderstorm caused the radar system to give a false reading.

Jeremy found a reference to it at

<http://www.bautforum.com/archive/index.php/t-9596.html>

It [trying physics to get out of a speeding ticket] was tried in Los

Alamos. One of the weaponeers was booked for driving his vehicle at speeds

well in excess of the limit. At his trial he produced an involved theory

of high-energy physics that suggested the radar speed gun readings were

distorted by a nearby thunderstorm. The judge's summation went.

"Only in Los Alamos would a defendant argue high-energy physics as a

defense against a charge of driving with excessive speed. Only in Los

Alamos would the Judge have the PhD necessary to know that he was talking

utter nonsense."

[Note: Steven J. Greenwald runs a low-volume mailing list intended to foster interaction between his former/current students from James Madison

University's graduate INFOSEC program (<http://www.infosec.jmu.edu>) and other

"security seniors" he knows either personally or by reputation. If you think you qualify and wish to request a subscription, please send e-mail to Steve with the e-mail address and name you wish to use. PGN]

✶ Gatwick Airport screens display wrong local time

<"Philippe Jumelle" <pjumelle@gmail.com>>

Mon, 29 Oct 2007 14:52:22 +0100

Quite surprisingly (except for RISKS readers), a daylight-saving glitch hit

Gatwick Airport on Oct 28th resulting in ire of passengers and relatives.

http://www.theregister.co.uk/2007/10/29/gatwick_computer_glitch/ and others

[Back at the beginning of April, I noted in [RISKS-24.63](#) that Caltrain

managed to botch the daylight saving cutover. This week they did it even

more curiously: the Menlo Park Station had the correct daylight time

displayed on one side of the tracks, and the week-too-early standard time

on the other side. On the other hand, it makes some sense that the two

sets of displays at any given station are intentionally controlled

separately, particularly when bearing the bad news of late trains

and accidents in one direction or the other. PGN]

✶TV PVRs getting BST change not quite right

<Nick Rothwell <nick@cassiel.com>>

Sun, 28 Oct 2007 16:23:09 +0000

Since it's the time of year for summer time/daylight savings bugs, here's mine, from the Humax PVR-9200T. It's a UK hard disk TV recorder which takes Freeview digital-over-aerial channels and supports a seven-day EPG (programme guide).

Yesterday (last day of BST), the programming timeline display showed continuous time across the BST-to-GMT boundary; programmes before the change showed the correct broadcast time, programmes after the change were lined up against time markers one hour ahead of the wallclock time at which they would actually be broadcast: in other words, everything was displayed in BST, so a 7pm weekly episode yesterday would be followed by an 8pm episode this coming Saturday. Today, all times are in GMT, including those of programmes before the time change.

So, I thought: a consistent, if slightly unexpected, view of time changes, and one which would allow the device to switch times unambiguously... except, of course, it doesn't work: programmed recording entries are apparently stored with clock times, so all the recordings I programmed last week will now start (and stop) one hour late. I'm currently going through and editing them all...

⚡ DST traffic signal snafu

<"D. Joseph Creighton" <djc@cc.umanitoba.ca>>

Mon, 29 Oct 2007 10:47:35 -0500

Monday 29 Oct 2007.

Hundreds of traffic lights in Winnipeg, Canada did not change from their overnight 'flashing amber' states to the normal 'morning rush' state until an hour later than usual due to old DST settings in them. The lights will need to be manually overridden for the week until time catches up.

Ref. <http://www.cbc.ca/canada/manitoba/story/2007/10/29/daylight-time.html>

The RISK of believing all your DST issues are fine when there's no problem in the spring is illustrated nicely here.

D. Joseph Creighton [ESTP] | Info. Technologist, Database Technologies, IST
Joe_Creighton@UManitoba.CA | University of Manitoba Winnipeg, MB, Canada, eh?

⚡ Who set up that meeting anyway?

<"Jeremy Epstein" <Jeremy.Epstein@softwareag.com>>

Mon, 29 Oct 2007 13:37:38 -0400

As many readers are aware, there's frequently a discrepancy between when

countries switch between "summer time" (or Daylight Savings Time as it's called in the US) and "winter time" (or Standard Time). Europe switched to winter time this year on Oct 28; the US switches to Standard Time on Nov 4. What I'm finding today is that my schedule is a shambles, because meetings that are normally sequential are overlapping, depending on who scheduled the meeting. As an example, I have a meeting I normally attend every Tuesday at 8:30 Eastern; because that was set up in Outlook by a colleague in Europe, this week it's at 9:30 Eastern (i.e., the time stayed constant for him but shifted for me). I have another meeting every Tuesday at 9:30 Eastern which contains an overlapping set of attendees, but because I set that one up, Outlook has left my time constant and shifted my European colleagues - thus, the two meetings "overlap".

Of course, they don't really overlap - it's an artifact of how we've become dependent on computerized scheduling systems without thinking about the implications. Yet another reason, I suppose, why airlines and military systems run on "Zulu time", so as to avoid these glitches!

✶ US Congress pulls the classic e-mail oopsie

<Danny Burstein <dannyb@panix.com>>
Sun, 28 Oct 2007 14:47:42 -0400 (EDT)

The House Judiciary Committee wrote back, via e-mail, to the contributors to

its confidential whistleblower Internet submission hotline.

Aside from the standard issues of doing any of this stuff via insecure and unverified e-mail, they listed all the e-mail addresses in the "to" line, so everyone saw everyone else's name [a].

One of the addresses they sent this whole list to was...
vice_president@whitehouse.gov [b]
ratcheting up the usual paranoia concerns.

lots more detail at:

<http://www.tpmmuckraker.com/archives/004576.php>

[a] since many e-mail spam filters will kill off material addressed to large numbers of recipients, many of the intended folk probably never got the note.

[b] it's unclear whether this was really the address they were using to send a copy to the VP or whether it was one of the "fake" ones used by initial submitters. I suspect it was the latter.

Either way this procedure was pretty clueless.

Who needs bots? (Re: Williams, [RISKS-24.87](#))

<Matt Simpson <net-news69@jmatt.net>>

Tue, 23 Oct 2007 11:19:05 -0400

In "Risks of cute e-mail" in [RISKS-24.87](#), Chris Williams says

> 1) Who needs a bot army to send spam/viruses when you can get people to

> willingly forward things along for you?
>
> 3) Since this appears to have started as a local phenomenon
and has slipped
> by every anti-spam and anti-virus engine, the potential for
malice is
> high.

There's a joke about the use of gullible humans instead of bots
to spread
viruses. It's an e-mail that says something like:

"This is the <insert favorite stupid ethnicity here> virus.
We don't have
any smart programmers, so please erase all the files on your
hard drive
and forward this to all your friends."

Haha. Very funny. What's really funny is that, if worded just
a little bit
differently, this can work, as has already been demonstrated.

Another popular legend that circulated for a while a few years
ago was the
"virus" that was on every Windows system. The e-mail warned of
some virus
that the sender had found on his own system. It gave
instructions for
browsing some directory deep within the bowels of Windows, and
if you found
a specific file name, that meant you were infected, and you
needed to delete
the file.

Of course, the file was one that exists on any normal Windows
system.
(Un)fortunately, it was something non-critical, so deleting it
didn't do
much damage, and restore instructions were widely available. I
actually
wished that those who followed the warning and deleted the file
had suffered
more damage as a result of their gullibility.

So, although the "redneck" virus was a joke, it really is possible to send people e-mail that will cause them to voluntarily delete parts of their operating system and then forward the mail to all their friends. Just don't include the word "joke" and they'll do it.

Re: Fake blogs (Yurman, [RISKS-24.86](#))

<Dan Jacobson <jidanni@jidanni.org>>

Wed, 24 Oct 2007 04:24:10 +0800

DY> The problem of fake blogs is significant for me...
DY> I have no way as an individual to stop the current problem...

Hold the domain owner responsible perhaps?:

Dear Yahoo Corporation, YOUR website, http:..., is impersonating MY website. Please cease and desist.

It would be wrong to go further and give YOU, the impersonators, copies of MY personal identification documents you request as proof of my identity. I'm sure you will agree.

YOU, Yahoo Corporation, are impersonating MY website. YOU are responsible!

Is that not MY telephone number on YOUR website? Call it!

Does YOUR page not say "This page should be at http:...? And where is that? MY website!

I demand YOU remove http:... It is an unauthorized copy of MY website!

Update: my above bold e-mail merely got me the same form e-mail from Yahoo asking for identification. The Federal Trade Commission website, where I turned to next, says they don't solve individuals' problems, which is just as well, as their webform produced an error.

Second update: No need to hide the URLs:

<http://www.geo.phony.cities.com/fireboy1983/index.htm>
impersonates my :real: <http://jidanni.org/>

⚡ Same ol' same ol'

<"Andrew Koenig" <ark@acm.org>>

Thu, 18 Oct 2007 10:54:20 -0400

Today I got e-mail from the bank that services one of my credit cards, saying:

Need to simplify your finances?
A Balance Transfer can help!

followed by various comments and a clickable link marked

TRANSFER BALANCES NOW

I was about to dismiss this as yet another phishing scheme, but I was surprised by how authentic it looked. Then I looked more closely, and noticed that it included my name (correctly spelled) and the last four digits of my account number.

So I checked the destination for the link, and it actually did

refer to my
bank's website. Not only that, but the two other hyperlinks in
the message
also referred to my bank's website.

... From which I can only conclude that this bank is trying to
train its
customers to be vulnerable to phishing scams. What on earth
could they be
thinking?



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 89

Friday 2 November 2007

Contents

- [Computer glitch stops TransAdelaide trains](#)
[Andrew Pam](#)
- [Predicting fatigue failure](#)
[Ken Knowlton](#)
- [Satanic car key traps 12 motorists in car park of horror](#)
[Chris Leeson](#)
- [Car park denial-of-service attack](#)
[Peter Houppermans](#)
- [Risk of Unanticipated Countermeasures -- Congestion Pricing](#)
[David Lesher](#)
- [License plate scanners in police cars](#)
[Jonathan de Boyne Pollard](#)
- [A second look at the Mac OS X Leopard firewall](#)
[Monty Solomon](#)
- [CAPTCHA trojan](#)
[Scott Nicol](#)
- [Mac trojan in-the-wild](#)
[Gadi Evron](#)
- [Double Dipping and Double Charging](#)
[Paul Robinson](#)
- [Re: Fighting traffic citations](#)
[Doug McIlroy](#)
- [Plagiarism & technology](#)
[Jeremy Epstein](#)
- [End of Leap Seconds?](#)
[Rob Seaman](#)
- [Info on RISKS \(comp.risks\)](#)

⚡ Computer glitch stops TransAdelaide trains

<Andrew Pam <xanni@glasswings.com.au>>

Fri, 02 Nov 2007 13:29:56 +1030

THE supplier of the problem-plagued \$9.5 million computerised Central Train System will be forced to fix it, as commuters were again delayed yesterday.

TransAdelaide general manager Bill Watson yesterday revealed an audit of the system was already in progress after it caused disruptions to morning services. "There has been a whole series of different problems," Mr Watson said. "They have diminished quite substantially, but there are still incidents once or twice a month which is unacceptable." The latest problem caused delays of up to 15 minutes for morning commuters from 6.30am yesterday, Mr Watson said. "The server became unstable and caused delays right across the network," he said. "By 10am everything was back to normal. The system had stabilised itself."

<http://www.news.com.au/adelaidenow/story/0,22606,21913481-5006301,00.html>

THE computer problem that threw the travel plans of about 15,000 rail commuters into chaos yesterday had been known to for almost five months.

An audit of the \$9.5 million computerised Central Train System was ordered by TransAdelaide in May and completed at the end of June. The same problem that created yesterday's chaos also caused disruptions to morning train services in June.

Thousands of passengers were stranded or delayed yesterday morning because of the ongoing technical problem with the computerised train control system. [...]

<http://www.news.com.au/adelaidenow/story/0,22606,22684078-5006301,00.html>

Andrew Pam <http://www.sericyb.com.au/>

⚡ Predicting fatigue failure

<Ken Knowlton <KCKnowlton@aol.com>>

Thu, 1 Nov 2007 11:22:34 EDT

Speaking from ignorance, I'll make this short. Many disasters (recently the Minneapolis bridge, in 2001 the Airbus 300 in Queens) are presumed to have resulted from fatigue failure. Without analyzing/guessing about possible modes of failure, couldn't one start with this low-knowledge, high-tech method: One at a time, tug together several (arbitrarily selected?) pairs of points of a structure, recording compliance curves. If the loading and

unloading curves don't match, or if they are different from last month's curves, something can be presumed to be happening. With the Queens Airbus: pulling tips of vertical and horizontal stabilizers together (presumably elastically) might have demonstrated changes over previous months. Is anything like this done? Even after-the-crash, such prior data would be valuable evidence -- exculpatory or otherwise. I've never heard of it.

✂ Satanic car key traps 12 motorists in car park of horror

<Chris Leeson <Chris.Leeson@atosorigin.com>>
Fri, 2 Nov 2007 12:01:46 -0000

The RISKS Archives are full of interference-related problems. Here's another one for the mix, related in **The Register**'s usual style.

http://www.theregister.co.uk/2007/11/02/kent_car_key/

12 cars in a Gravesend, Kent, car park failed to start or had alarms triggered by a faulty transmitter in another car. There had been problems in the car park for some time.

Not computer related? Well, the initial suspects were "a rogue transmitter or wireless broadband". Now that virtually everything appears to be wi-fi/bluetooth enabled these days, we can only expect more of the same.

✂ Car park denial-of-service attack

<Peter Houppermans <phobos@pobox.com>>
Fri, 02 Nov 2007 10:36:27 +0100

[... After quite a long search, the problems were found to emerge from a small family car which was alleged to send out signals blocking keyfobs in a 50m radius.

I must admit I have trouble believing that a CAR does this. Maybe something IN the car, but why would a mechanism in a car transmit? For what purpose? Main RISK: if someone works out how, I would find it's a major worry for any executive driver.

http://news.bbc.co.uk/2/hi/uk_news/england/kent/7073935.stm

✂ Risk of Unanticipated Countermeasures -- Congestion Pricing

<David Lesher <wb8foz@panix.com>>
Fri, 2 Nov 2007 01:25:21 -0400 (EDT)

Niraj Sheth, London's Congestion Fee Begets Pinched Plates,
*Wall Street Journal, 2 Nov 2007, B1
http://online.wsj.com/article/SB119396467957679995.html?mod=fpa_editors_picks

London's congestion pricing for drivers is heralded around the world for reducing traffic and pollution. It's also causing an unintended effect: a sharp jump in thieves stealing or counterfeiting license plates.

Thieves are pinching plates by the dozens every day to fool the city's traffic cameras, which enforce the £8 (\$16) daily charge to drive in central London as well as other traffic infractions. A computer system matches the plate numbers caught on camera with a register of vehicles; if owners don't pay a congestion fee (which they can do online, by phone or at gas stations) by the following day, they get a photo of their car along with a fine in the mail. With someone else's license plate on their car, scofflaws can drive around free, and any fines are billed to the plate's rightful owners.

Before the congestion charge took effect in February 2003, police didn't bother to track stolen number plates, as they're called in Britain, because so few incidents were reported. In 2004, nearly 6,000 plates were stolen, according to London's Metropolitan Police. Reports of stolen plates in the city spiked to 9,777 last year. Up to 300 cars with illegal license plates enter London's congestion charge area every day, according to the country's Automotive Association.

Where IS James Bond's Aston Martin DB5 when you need it?
Caught in traffic, no doubt...

⚡ License plate scanners in police cars (McCool, [RISKS 24.86](#))

<Jonathan de Boyne Pollard <J.deBoynePollard@Tesco.NET>>
Fri, 02 Nov 2007 10:28:36 +0000

> The article briefly mentions that such systems are common in London and in
> casinos, with little discussion of any problems that may have come up.

In fact, ANPR (Automatic Number Plate Recognition) has quietly become all-pervasive in the U.K. in recent years. (Fitch pointed out the construction of a national ANPR network two years ago in [RISKS 24.09](#). ANPR-equipped vehicles are almost permanent fixtures in some places, also.) M. McCool's observation that "the enthusiasm for the systems in this article is tangible" can be repeated for much news coverage of the subject, where there is great emphasis on the "security" and "safety" of having automatic cameras and picture recognition softwares linked to various databases of the

country's population.

In part that enthusiasm can be traced back to originating with the news sources themselves, whose interests in downplaying any potential for abuse, accident, or error in these systems are understandable. A quick Google News search turns up many articles, such as

<URL:http://news.bbc.co.uk/2/hi/uk_news/england/bristol/somerset/7037938.stm>,
 <URL:http://news.bbc.co.uk/2/hi/uk_news/magazine/7048645.stm>,
 <URL:<http://www.wbtimes.co.uk/content/brent/willesdenchronicle/news/story.aspx?brand=WBCOnline&category=news&tBrand=northlondon24&tCategory=newswbc&itemid=WeED04%20Oct%202007%2017%3A51%3A27%3A037>>,
 <URL:http://www.thisislancashire.co.uk/news/headlines/display.var.1745860.0.caught_on_camera.php>,
 <URL:http://manchestereveningnews.co.uk/news/s/1017764_cops_crush_10000_cars>,

many of which are quick to tout the numbers and categories of arrests made, and how many vehicles were impounded, and gloss over or ignore questions of whether any errors were made. Such coverage has all the trappings of journalists simply regurgitating press handouts. (Compare the aforelinked BBC News coverage with that of another news organization at <URL:http://gazetteseries.co.uk/mostpopular.var.1760672.mostviewed.arrests_at_operation_on_bridge.php>, for example.)

The cited statistics also require some scrutiny. The Manchester Evening News article, for example, repeats police claims that "uninsured drivers are six times more likely to have convictions for driving un-roadworthy vehicles and nine times more likely to have convictions for drink-driving". But the thought that immediately comes to mind is how much that disparity might simply be an artifact of the way that the statistics are gathered. Whether a driver has insurance is only checked after he has already been stopped for another reason. There is, as yet, no automatic roadside system for scanning drivers as they pass and checking them against the central MIB (Motor Insurers' Bureau) database to see whether they have insurance. The measured ratio of uninsured to insured drunk drivers may be 9:1 (which seems to be the datum that the claim is derived from). But that may simply be because there are many uninsured drivers who are not stopped for drunk-driving.

There is an interesting 2005 editorial piece in The Register at <URL:http://www.theregister.co.uk/2005/03/24/anpr_national_system/> on this subject, which discusses the problems of directly checking whether drivers are insured. But perhaps the most interesting article related to this is Neil Mackay's 2007-10-06 article in The Sunday Herald at <URL:<http://sundayherald.com/news/heraldnews/display.var.1741454.0.0.php>>.

Two quotes stand out from it. The first is the first line of the report being discussed: "We live in a surveillance society." The second is from the information commissioner, Richard Thomas: "Today, I fear that we are, in fact, waking up to a surveillance society that is already all around us."

The report discussed by Mackay depicts a dystopian vision of the U.K. in 2017. Some may dismiss such visions. Science fiction is littered with

disturbing visions of the future that have never come to pass, after all; and the regularity of that may lead some to erroneously think that all such predictions are, similarly, unlikely to be realized. However, science fiction is also littered with occasions where fiction became fact. One relevant example: The police hoverdrones of the television series Dark Angel, set in the U.S. in 2019, are to become a reality in the U.K. in 2007/2008 according to

<URL:<http://www.scenta.co.uk/Gadgets/1707394/silent-witness.htm>>.

✂ A second look at the Mac OS X Leopard firewall (Jürgen Schmidt)

<Monty Solomon <monty@roscom.com>>

Tue, 30 Oct 2007 22:36:30 -0400

Jürgen Schmidt, Leopard with chinks in its armour, 29 Oct 2007

Apple is using security in general and the new firewall in particular to promote Leopard, the latest version of Mac OS X. However, initial functional testing has already uncovered cause for concern.

The most important task for any firewall is to keep out uninvited guests. In particular, this means sealing off local services to prevent access from potentially hostile networks, such as the Internet or wireless networks.

But a quick look at the firewall configuration in the Mac OS X Leopard shows that it is unable to do this. By default it is set to "Allow all incoming connections," i.e. it is deactivated. Worse still, a user who, for security purposes, has previously activated the firewall on his or her Mac will find that, after upgrading to Leopard, the system restarts with the firewall deactivated.

In contrast to, for example, Windows Vista, the Leopard firewall settings fail to distinguish between trusted networks, such as a protected company network, and potentially dangerous wireless networks in airports or even direct Internet connections. Leopard initially takes the magnanimous position of trusting all networks equally. ...

<http://www.heise-security.co.uk/articles/98120>

✂ CAPTCHA trojan

<Scott Nicol <scott.nicol@gmail.com>>

Fri, 02 Nov 2007 15:08:53 -0400

Interesting blog entry at Trend Micro on a new "striptease" trojan,

that's simply a ploy to get users of the trojan to solve CAPTCHAs:

<http://blog.trendmicro.com/captcha-wish-your-girlfriend-was-hot-like-me/>

Nice to see that we've progressed from the thin-client model of a few years ago ([RISKS-23.17](#)) to today's more robust client implementation.

⚡ Mac trojan in-the-wild

<Gadi Evron <ge@linuxbox.org>>

Wed, 31 Oct 2007 18:23:23 -0500 (CDT)

For whoever didn't hear, there is a Macintosh trojan in-the-wild being dropped, infecting mac users. Yes, it is being done by a regular online gang--itw--it is not yet another proof of concept. The same gang infects Windows machines as well, just that now they also target macs.

<http://sunbeltblog.blogspot.com/2007/10/screenshot-of-new-mac-trojan.html>

<http://sunbeltblog.blogspot.com/2007/10/mackanapes-can-now-can-feel-pain-of.html>

This means one thing: Apple's day has finally come and Apple users are going to get hit hard. All those unpatched vulnerabilities from years past are going to bite them in the behind.

I can sum it up in one sentence: OS X is the new Windows 98. Investing in security ONLY as a last resort losses money, but everyone has to learn it for themselves.

[Mike Hogsett's reaction to this: "Sure, it is a vulnerability, but the user has to confirm the download, then run the installer, then enter their admin name and password during the installation of the trojan. PGN]

⚡ Double Dipping and Double Charging

<Paul Robinson <paul@paul-robinson.us>>

Sat, 27 Oct 2007 03:35:35 -0400

In [RISKS-24.86](#), Arthur Flatau mentions how the Austin, Texas tollway system is double-billing some customers. And that it seems odd they couldn't have designed the system to ignore duplicate transponders occurring very close to each other.

On this point, I agree. Even if someone was able to make a duplicate of a transponder, I think it would be extremely unlikely that they would use it

on two vehicles traveling together. Now, two people, on the other hand, might be a different story. So I have a different story.

Back, oh, about twenty years ago I lived in Long Beach, California, Long Beach Transit, the local bus company, went from the old "dump" style fareboxes to the fully automatic ones that count the money and even have a magstripe reader, so they changed from a regular paper-type bus pass to one with a mag strip. You would swipe your monthly pass through the reader and it would beep. If something was wrong, it would beep twice and the display would tell the driver what it was. (I was a cash payer because a pass didn't work for me; I had to use two different bus companies to get to work, and they didn't accept each other's passes.)

So I got thinking about it, and I was talking to a driver, and I asked him what would keep someone traveling with someone else from sneaking their pass back, say, out the window to someone else (I have seen it done by kids on the bus sometimes, if they're slick about it the driver will never know!) He said that it doesn't allow it. He asked me to wait until the next person came on with a pass and he'd show me.

So, a few stops later someone came on and swiped their pass through, and it beeped once. He asked the woman if she would do it again, and she did. It beeped twice, and on the LCD display I could see it said "PASSBACK". (I was, at the time, sitting in the seat directly behind the driver.) The driver explained to me that it won't let you use the same bus pass on that bus for about ten minutes.

So, twenty years ago the technology on a bus farebox was capable of knowing when an access token was being used twice, but even with the advances in technology we can't do it today. On the other hand, it could be argued that there's no percentage in keeping you from cheating the customers but a lot of incentive in preventing the customers from cheating you, so maybe that's part of the reason.

Paul Robinson <http://paul-robinson.us> - My Blog

✂ Re: Fighting traffic citations ([RISKS-24.88](#))

<Doug McIlroy <doug@cs.dartmouth.edu>>
Wed, 31 Oct 2007 20:22:54 -0400

"Fighting traffic citations", 26 October 2007, brought to mind an old Joe Condon story. Seems his neighbor was hauled in for speeding in his Porsche and asked if Joe might be able to check the accuracy of the radar. Joe relished the challenge and agreed to serve as an expert witness. He borrowed the very radar from the police and set it up at the very spot of the ticket, where the cop lurked just where cars came into view around a wooded curve. The radar worked fine on several trials at the speed limit and then gave a startlingly high reading. A truck appeared out of the woods

behind the Porsche; its big cross-section had been detected through the trees beyond the little stealth car. Joe testified to this at the trial, but his neighbor was found guilty anyway. After the trial the judge took them aside and told them what technicalities to appeal on. He had been willing to accept Joe's evidence that the radar might have detected a following vehicle, but was unwilling to get that fact recorded as a precedent.

✈️ Plagiarism & technology

<Jeremy Epstein <Jeremy.Epstein@softwareag.com>>

Mon, 29 Oct 2007 12:25:23 -0400

The interaction of plagiarism and technology seems to crop up periodically in the news, and at PGN's invitation I'm writing this brief note in hopes of soliciting a discussion. A recent discussion on the USACM (Public Policy Committee of the Association for Computing Machinery) mailing list triggered these thoughts. I'm also posting this on my blog in case anyone feels like adding comments there. (<http://abgordia.blogspot.com>)

It's obvious that the availability of so much information online makes plagiarism easier - it's impossible for a reader to know everything that could have been used without permission or attribution. On the flip side, things like Google make it easier to find suspected instances - as an example, when I'm reviewing an article for a journal or conference, I frequently put phrases in to Google that I suspect are stolen, and have on numerous instances found that they were in fact taken verbatim without attribution. [Hint to the plagiarist: if you're going to use someone else's words without attribution, make sure they fit with your writing style. This is particularly notable when choosing text written by someone with a different native language than your own - if your native language is English and you copy something written by a native Chinese speaker, it will be fairly obvious; the converse is also obviously true.]

For high school and college students, technology like TurnItIn (www.turnitin.com) is one way of finding plagiarism without teachers having to do extensive searching. Although I haven't personally seen the output, my understanding is that the student submits text which is automatically analyzed, and potential instances of plagiarism are noted in a message to the teacher. (If someone could provide a better explanation, I'd certainly appreciate it! I noticed that TurnItIn now put emphasis on improving students' writing style, perhaps as a way to give students a feeling that they're getting something out of the deal.)

There are several problems with products of this sort:

(1) False positives. When my daughter was in high school, she noted several times that TurnItIn considered her a plagiarist because it was unable to distinguish between properly quoted/referenced text, and unauthorized

copying. Teachers who simply look at the overall "score" without reading the individual comments will tend to penalize those students who do the best job of citing background work! (I'm reasonably sure that TurnItIn is sufficiently cautious as not to deny that there are false positives, and to strongly encourage teachers and students to examine the results rather than simply believing them verbatim.)

(2) Copyright infringement. TurnItIn keeps copies of student papers in their database, for matching against future papers. This seems reasonable at first blush - after all, selling term papers is an old tradition, dating back well before the Web (although today's students may not believe that)! However, by keeping submissions for matching, TurnItIn may be violating copyright, as a recent lawsuit claims (see "McLean Students Sue Anti-Cheating Service", Washington Post, March 29 2007, <http://www.washingtonpost.com/wp-dyn/content/article/2007/03/28/AR2007032802038.html>). Additionally, students have effectively no option to refuse adding their papers to the database, and are not compensated for their submissions.

So to bring this to RISKS, the issue is that we have competing risks: the risk of plagiarism being combated by TurnItIn and similar products vs. the risk of unfair accusations of plagiarism and copyright infringement - all of which is enabled by technology.

🚩 End of Leap Seconds? (Re: [RISKS-24.79](#))

<Rob Seaman <seaman@noao.edu>>

Thu, 25 Oct 2007 13:43:30 -0700

An earlier thread, "U.S. legal time changing to UTC" discussed a possible future for UTC without leap seconds. We are now just one step away from that future. Rob Seaman, National Optical Astronomy Observatory

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

From: Richard B. Langley
To: Canadian Space Geodesy Forum
Subject: End of Leap Seconds?

At the Civil GPS Service Interface Committee meeting in Fort Worth last month, Dr. Wlodzimierz Lewandowski from the Bureau International des Poids et Mesures (BIPM) summarized the outcome of the International Telecommunication Union (ITU) meeting on the redefinition of Coordinated Universal Time (UTC), which was held in Geneva, 11-14 September 2007:

- o April 2008: ITU Working Party 7A will submit to ITU Study Group 7 project recommendation on stopping leap seconds
- o During 2008, Study Group 7 will conduct a vote through mail among member states

- o 2011: If 70% of member states agree, World Radio Conference will approve the recommendation
- o 2013: Application of leap seconds will stop and UTC will become a continuous time scale.

The risk here is in attempting to resolve a technological issue with complex implications by voting. One would submit that any solution that generates a negative opinion from 30% of a pool of experts is a bad solution. Worse yet is if the voters are not themselves experts...

Rather, a coherent plan should be developed in an open, collaborative environment and a consensus should be sought not only to the acceptability of the plan, but to its necessity. Participation should be sought from all affected communities - that list is quite extensive for timekeeping. For instance, one might expect a UTC conference to be organized, not just an internal meeting of the ITU.

In this case, no plan whatsoever exists for addressing the inevitable discontinuity that will occur as the missing leap seconds accumulate. The previous thread described why civil time is a flavor of mean solar time in the first place. What happens when this assumption is challenged?

Earlier suggestions for embargoing leap seconds relied on the flabby idea of leap hours. The leap hour concept appears to rest on the notion that many localities manage to handle one hour Daylight Saving Time shifts twice a year. Perhaps the thought is simply that a year will come when one of the DST jumps is skipped...unfortunately, it doesn't work like that. (And not only because not all localities observe DST, and not all at the same time.) The precise reason that DST is an acceptable timekeeping policy is that any civil or legal entities or systems that need to know an unambiguous time can fall back on a common worldwide UTC. It would be completely inappropriate to institute a leap in UTC by resetting the clocks to run through the same hour twice. How could one disambiguate that hour of world history ever after?

Rather, a leap second is an intercalary event like a leap day - that particular minute, hour, and day is one second longer. There is no ambiguity during a leap second. A leap hour would simply be 3600 embargoed leap seconds released one after another. That particular red-letter day would have 25 hours. Any software that has trouble handling the time 23:59:60 would be faced with 3600 such time values in a row: 24:00:01, ..., 24:59:59, 25:00:00.

But that's not all, since the leap hour would occur all over the world at the same time. The leap second 2005-12-31T23:59:60 corresponded to 18:59:60 EST in New York City and 15:59:60 PST in Los Angeles. A leap hour, say 2600-12-31T24:00:00-24:59:59, would be interposed between the successive clock ticks 18:59:59 and 19:00:00 in New York, between 15:59:59 and 16:00:00 in LA.

How would this work logistically? For instance, would the NYC clock count from 18:59:60 to 18:59:3659? This is the sort of detail that should be

worked out before voting a fundamental change to UTC.

Rob Seaman, National Optical Astronomy Observatory, Tucson, AZ



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 90

Tuesday 6 November 2007

Contents

- [Computer Glitch Rolls Back Provincial Government](#)
[Ken Dunham](#)
- ["Error" blitzes health records in New Zealand](#)
[Robert S. Heuman](#)
- [UK Revenue loses CD-ROM](#)
[Bernhard Riedel](#)
- ["Network Neutrality Squad": Users Protecting an Open and Fair Internet](#)
[Lauren Weinstein](#)
- [Technology, the Stealthy Tattletale](#)
[Christopher Maag via Monty Solomon](#)
- [GPS Units With More to Say](#)
[Roy Furchgott via Monty Solomon](#)
- [Zombie botnet spam attack from over 3,000 IP addresses in 8 hours](#)
[Jonathan Kamens](#)
- [Problems with Google's Spam filters and Google Content](#)
[Terence Eden](#)
- [Spelling corrector creates "Muttonhead Quail Movement"](#)
[PGN](#)

- [Cellphone in USB charger became default route](#)
[Stefan Alfredsson](#)
 - [Time change problems: Alltel](#)
[Steven M. Bellovin](#)
 - [Broken by design](#)
[Aahz](#)
 - [Update to "Think before you legislate"](#)
[Robert S. Heuman](#)
 - [Re: Predicting fatigue failure](#)
[Gary Maxwell](#)
 - [Re: Mac OS X Leopard firewall](#)
[Chris Adams](#) [Ted Lemon](#)
 - [Re: Plagiarism & technology](#)
[Bob Brown](#)
 - [Re: "Same ol' same ol'"](#)
[Eric Ball](#)
 - [Re: Leaping onward](#)
[Rob Seaman](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Computer Glitch Rolls Back Provincial Government**

<"Ken Dunham" <kdunham@rogers.com>>

Thu, 1 Nov 2007 12:27:51 -0400

Anyone surfing the New Brunswick government website on 1 Nov 2007 might have

wondered if the province's former Conservative government had staged a coup.

A computer glitch posted the week's agenda for Premier Bernard Lord and a

news conference on pandemic planning with Health Minister Elvy Robichaud.

However, neither man is still in office.

It turns out a faulty computer server spit out information for

January 2006

-- well before the Tories were defeated in the last provincial election and

replaced by Premier Shawn Graham and his Liberal government.

Technicians

are trying to trace the problem. [Source: Canadian Press item, 1 Nov 2007]

http://ca.news.yahoo.com/s/capress/071101/technology/technology_oddity_computer_glitch

⚡ "Error" blitzes health records in New Zealand

<"Robert S. Heuman" <robert.heuman@alumni.monmouth.edu>>

Sat, 03 Nov 2007 11:38:11 -0400

This is what happens when there is NO full OFF-SITE back-up available! Bob

As a result of two disks failing on 21 Oct 2007, thousands of hours' work

over many years on the part of 690 staff members at the Waikato District

Health Board has vanished after a major computer error at Waikato Hospital.

The lost data -- which includes countless e-mails and personal work files,

reports, letters, communications, teaching material, guidelines -- was

information that was backed-up in the hospital's storage area network. The

hospital is spending at least \$60,000 trying to retrieve the information and

has hired experts in the US. [Source: Natalie Akoorie, Error blitzes health

records, *Waikato Times* 3 Nov 2007; PGN-ed]

<http://www.stuff.co.nz/4260645a11.html>

[Also noted by Andrew King in the NZ Herald. PGN]

UK Revenue loses CD-ROM

<"Bernhard Riedel" <bernhard@sdg.de>>

Sat, 3 Nov 2007 20:48:26 +0100 (CET)

"Thousands at risk after data loss"

<http://news.bbc.co.uk/2/hi/programmes/moneybox/7076106.stm>

A CD-ROM containing personal details about some 15000 people was lost by a

courier. I remember a time when such stuff was moved on magtapes in huge

aluminum boxes, not as easy to mislay, I guess.

Risks of miniaturization?

One really intriguing thing here (for me):

The Revenue refused to say "on security grounds" whether the information was encrypted.

Does anybody have a plausible idea what kind of security grounds that might be?

Bonus:

"Dog starts car after eating chip"

http://news.bbc.co.uk/2/hi/uk_news/england/southern_counties/5382878.stm

This one shows that new technology can cause not only unintended new failure modes, but also new modes of recovery from failures.

[Perhaps the dog thought it was a BONE-US. PGN]

🚀 "Network Neutrality Squad": Users Protecting an Open and Fair Internet

<Lauren Weinstein <lauren@vortex.com>>

Mon, 05 Nov 2007 16:49:47 -0800

"Network Neutrality Squad": Users Protecting an Open and Fair Internet

<http://lauren.vortex.com/archive/000327.html>

Greetings. I'm very pleased to announce a new project from PFIR - People For Internet Responsibility:

"Network Neutrality Squad" - NNSquad

<http://www.nnsquad.org>

PFIR Co-Founders Peter G. Neumann and I are joined in this announcement by Keith Dawson (Slashdot.org), David J. Farber (Carnegie Mellon University), Bob Frankston, Phil Karn (Qualcomm), David P. Reed, Paul Saffo, and Bruce Schneier (BT Counterpane).

Recent events such as Comcast's lack of candor regarding their secretive disruption of BitTorrent protocols, and Verizon's altering of domain name lookup results to favor their own advertising pages, are but tip-of-the-iceberg examples of how easily Internet operations can be altered in ways that may not be immediately obvious, but that still can have dramatic, distorting, and in some cases far-reaching negative consequences for the Internet's users.

The Network Neutrality Squad ("NNSquad") is an open-membership, open-source

effort, enlisting the Internet's users to help keep the Internet's operations fair and unhindered from unreasonable restrictions.

The project's focus includes detection, analysis, and incident reporting of any anticompetitive, discriminatory, or other restrictive actions on the part of Internet service Providers (ISPs) or affiliated entities, such as the blocking or disruptive manipulation of applications, protocols, transmissions, or bandwidth; or other similar behaviors not specifically requested by their customers.

Other key aspects of the project are discussions, technology development and deployment, and associated activities -- fostering cooperation and mutually agreeable methodologies whenever possible -- aimed at keeping the Internet a maximally unhindered, useful, competitive, fair, and open environment for the broadest possible range of applications and services.

We invite individual, commercial, nonprofit, government, and all other Internet users and stakeholders (including ISPs) to participate in the Network Neutrality Squad.

Please join the moderated mailing list (choice of immediate distribution or digest) for project announcements and discussions,

by sending a message (any subject or text) to:

`nnsquad-subscribe@nnsquad.org`

or by signing up at the mailing list Web page:

<http://lists.nnsquad.org/mailman/listinfo/nnsquad>

A moderated, interactive discussion and incident reporting forum is also available for more real-time communications on related topics:

<http://forums.pfir.org/main/messages/714/714.html>

Questions and comments are welcome at nnsquad-info@nnsquad.org, or feel free to contact me directly for details.

Working together, we can help to keep the Internet an incredibly useful resource for everyone around the globe, unhampered by any efforts to skew its enormous capabilities in ways that could hinder the many while benefiting the relative few.

We hope that you'll join this cause. Thank you for your consideration.

(Affiliations shown for identification purposes only.)

Lauren Weinstein <http://www.pfir.org/lauren> lauren@vortex.com
Tel: +1 (818) 225-2800 Lauren's Blog: <http://lauren.vortex.com>
People For Internet Responsibility - <http://www.pfir.org>
Founder, PRIVACY Forum - <http://www.vortex.com>

⚡ Technology, the Stealthy Tattletale (Christopher Maag)

<Monty Solomon <monty@roscom.com>>

Fri, 2 Nov 2007 23:34:21 -0400

After stealing \$7,000 from a PNC Bank in Evendale, Ohio, Kenneth Maples climbed into a white Ford pickup driven by his wife, Jewell, according to a police report. ... But the suspects never had a chance. A Global Positioning System tracking device had been tucked inside the stolen cash,

according to the report, allowing a small army of local police officers and F.B.I. agents to follow the signal from on-ramps and overpasses as it moved south into downtown Cincinnati. [Source: Christopher Maag, Tracking Thieves, or Teens: Technology, the Stealthy Tattletale, *The New York Times*, 27 Oct 2007; PGN-ed]
<http://www.nytimes.com/2007/10/27/technology/27tracking.html?ex=1351137600&en=8d6b9fafbd080801&ei=5090>

GPS Units With More to Say (Roy Furchgott)

<Monty Solomon <monty@roscom.com>>
Fri, 2 Nov 2007 23:36:58 -0400

The most advanced attempt at dynamic content is currently being made by Dash Navigation, whose portable GPS device not only receives positioning signals from satellites, but also collects driving speed and road data from cars that use it and anonymously report this information to a database. That data would let Dash know the actual speed at which traffic travels at different times of the day, so that it could route cars more effectively than current systems can. But for the Dash to build the database, it needs many drivers to buy the things and use them. [Source: Roy Furchgott, *The New York Times*, 24 Oct 2007; PGN-ed]
<http://www.nytimes.com/2007/10/24/automobiles/autospecial/24gps.html>

🔥 Zombie botnet spam attack from over 3,000 IP addresses in 8 hours

<Jonathan Kamens <jik@kamens.brookline.ma.us>>

Tue, 06 Nov 2007 02:21:27 -0500

This may be old news to some, but it was rather surprising to me, so I thought I'd pass it on...

At around 3:21pm US/Eastern on November 4, 2007, a zombie botnet began a dictionary spam attack against one of the domains I host.

zombie botnet --- a group of PCs that have been broken into by a hacker and turned into "zombies," i.e., PCs over which the hacker now has control, so that he can tell them to do things like send out spam on his behalf.

dictionary spam attack --- an attempt to deliver spam to legitimate users at a particular domain by attempting to send email to many different addresses within the domain in the hope that some of them will be valid.

I knew this was happening because the log monitor I run on my mail server began reporting many "User unknown" mail delivery failures for this domain every minute.

If this has been a typical dictionary spam attack coming from a single host, it would have been quickly blocked by my fail2ban <<http://www.fail2ban.org/>>

configuration, which temporarily bans any host which attempts a few failed SMTP deliveries within a short period of time. However, since the delivery attempts were coming from many different IP addresses all over the world, fail2ban was powerless to stop them.

When I realized what was going on, I wrote a script to block all the IP addresses from which invalid deliveries to the domain had been attempted, and I set up the script to run frequently to block any new IP addresses that turned up.

The attack continued until around midnight, i.e., for over eight hours.

During that time, I saw failed delivery attempts from 3,025 different IP addresses, along with 815 delivery attempts from IP addresses that I had already blocked.

At this point, I have two outstanding questions about this attack:

1. Was it really a dictionary spam attack, or was it actually a denial-of-service attack of some sort? I consider the latter a possibility because the email addresses to which delivery was attempted during the attack simply do not look like email addresses that someone would guess if they were seriously trying to get email through to a domain. Here are some examples of the addresses that were attempted: Lundberghrpor, Lanhamypxg, zsgohuwrhykr, CLIFFORDforonda, Lange, ThreeRiojas, Witold-Johannesen, birtlesioiis, Djurkovicnyqz, NevenHeinritz.

2. Is there anything productive I can do with the list I now

have of

the IP addresses over 3,000 compromised PCs? Is there a site somewhere to which I can submit the list that will notify the

appropriate network service providers about compromised PCs on

their networks? Is there any point in doing that? I suppose I

could write a script to run "whois" on each of the IP addresses,

try to parse out the contact email addresses, and send a form

letter to those addresses, but (a) I don't really have the time,

and (b) I believe that multiple whois queries from a single host

are throttled, so it would take me an awful long time to get

through them all.

⚡ Problems with Google's Spam filters and Google Content

<"Eden, Terence, VF UK - Technology" <Terence.Eden@vodafone.com>>

Thu, 1 Nov 2007 14:23:57 -0000

Over the last few months, I've noticed an increase in unfiltered spam within my GoogleMail inbox.

The spam - usually for online pharmacies - falls into two characteristics.

1) A sales pitch pointing to a Google Pages website e.g.

<http://12312.googlepages.com>

2) A sales pitch pointing to a Google Search e.g.

<http://www.google.co.uk/search?q=somestring>

The string that is passed to Google is usually the name of the pharmacy, ensuring that the spammer is in the top or the returned rankings. However, many spammers are using a "Googlehack" - a unique string - to ensure that their page is the **only** one that is returned.

The risks are two fold. Google's spam filter seems to trust "Google" content disproportionately.

Users may trust their search engine to provide clear and unbiased results, they may not expect that a search engine can be so easily bamboozled.

<http://www.google.co.uk/search?q=terence+Novarra+betavine>

✶ Spelling corrector creates "Muttonhead Quail Movement"

<"Peter G. Neumann" <neumann@csl.sri.com>>
Tue, 6 Nov 2007 13:17:34 PST

"Pakistan city virtually shut down after strike call. The opposition blames the government and the pro-government Muttonhead Quail Movement (MQM), which runs Karachi, for the violence."

[Someone noted that MQM actually stands for "Muttahida Quami Movement".]

["This is possibly the most unfortunate spell-check blunder I've ever seen. We corrected it: GBU Editor"]

[From Reuters blogs, filed by The Good, the Bad, & the Ugly

Editor (GBU),

14 May 2007; PGN-ed; thanks to Charles C. Mann for spotting it.]

<http://blogs.reuters.com/blog/2007/05/14/muttonhead-quail/>

✶ Cellphone in USB charger became default route

<Stefan Alfredsson <Stefan.Alfredsson@kau.se>>

Mon, 5 Nov 2007 09:55:50 +0100

His cellphone charger was broken, so 17 year old Christoffer connected his phone, a Sony Ericsson k800i, via USB to his parents computer and left it to charge over night.

A month later, he got a bill of SEK 6911 (about USD \$1100).

It turns out that the phone became the "default broadband" when plugged in via USB, and his long-running downloads were done over the phone instead of his broadband connection. The common price per Mbyte GPRS/UMTS data traffic is SEK 10 to 15 (about USD \$1.5 to \$2.3), which would correspond to about 500 Mbyte downloaded data.

Christoffer claims "there was no warning to allow the phone to take over the connection. I did not even know it was possible". According to the operator Tele2, he must pay the bill even if it was a mistake. They concluded that the phone modem had been used, but could not tell how it happened. The operator were not aware of previous incidents, but claims that "there is

software to link the phone to the computer and start the phone Internet function, but it's not possible for the computer to do this on its own".

Original article in Swedish:

<http://www.aftonbladet.se/goteborg/article1141706.ab>

⚡ Time change problems: Alltel

<"Steven M. Bellovin" <smb@cs.columbia.edu>>

Mon, 5 Nov 2007 02:37:35 +0000

We see reports like this twice a year, with some variation in timing because of different cut-over days in different countries. This time, Alltel -- a mobile phone company -- reported that some of its customers saw the time on their phones move forward an hour instead of back.

<http://ap.google.com/article/ALegM5idDfj-VyOMd0rsD0UlwSxGaIMLwD8SN4B001>

Steve Bellovin, <http://www.cs.columbia.edu/~smb>

⚡ Broken by design

<Aahz <aahz@pythoncraft.com>>

Sun, 4 Nov 2007 20:26:56 -0800

After reading RISKS for more than a decade, it takes **a lot** to shock me.

Here's "a lot" (lightly edited for name-hiding):

Date: Sun, 04 Nov 2007 17:24:49 -0500
From: Modest Needs Technical Support <tech@modestneeds.org>
To: Someone <foo@bar.baz>
Subject: Re: Modest Needs - Technical

Dear Someone,

Since we only allow one account per household, we've merged everything under your partner's (Aahz) account. Please ask him/her for the login information.

I hope this helps. Please write back if you still need technical support.

Sincerely,

Thierry Mellon, Chief Information Officer

Modest Needs is a charitable foundation that supplies short-term loans to people in sudden need. I've been donating to them for several years now, but given their unwillingness to use a sane security system, I shan't in the future. (We have received additional messages that communicate quite clearly that they have no intention of fixing this.)

Aside from the obvious RISKS about sharing passwords and financial information even for people who are partnered, what if Someone was just my roommate? Under what sane account-management regime do you simply merge accounts without asking permission?

✶ Update to "Think before you legislate" ([RISKS-24.88](#))

<"R.S. (Bob) Heuman" <robert.heuman@alumni.monmouth.edu>>

Fri, 02 Nov 2007 20:03:56 -0400

The Conservative government introduced a bill on Friday aimed at fixing a glitch in the Elections Act that could have prevented up to a million rural residents from voting... The bill introduced Friday clarifies that addresses do not need to contain a street name and number. CBC News, 2 Nov 2007

⚡ Re: Predicting fatigue failure

<"Gary Maxwell" <gmaxwell@casabi.com>>

Fri, 2 Nov 2007 18:31:28 -0700

Ken Knowlton's musings on real-world stress testing of in-service systems reminded me of a missed opportunity some years ago.

On Sunday, May 24, 1987, in celebration of its 50th anniversary, the Golden

Gate Bridge District closed down the bridge and allowed pedestrians to roam

freely on the span. The District estimates that nearly 300,000 people

"surged" onto the roadway. Clearly, the weight of shoulder-to-shoulder

people is much more than bumper-to-bumper traffic, and on this day, the

slight upward arch on the bridge's roadway actually flattened under the

weight. However, engineers did not anticipate this scenario, and the bridge

had not been instrumented to record the stresses encountered on

this
day. The Center for Design Informatics at the Harvard Design
School wrote a
paper evaluating the stresses, but this effort would have been
surely helped
by empirical data.

⚡ Re: Mac OS X Leopard firewall (Schmidt, [RISKS-24.89](#))

<Chris Adams <chris@improbable.org>>

Fri, 2 Nov 2007 16:29:29 -0700

This argument and the similar argument regarding wifi encryption
comes up
fairly often, which worries me because they're founded on an
implicit
assumption that network-specific security policies are a good
idea. We have
a mountain of evidence demonstrating that trusting any network
is a bad idea
because of rogue/unmanaged clients, malware and the difficulty
of ensuring
that the actual network setup faithfully conforms to policy.

Things like the TJX disaster demonstrate just how costly it can
be assuming
that it's ever safe to use applications which depend on network-
level
security rather than incorporating security into the application
itself. In
contrast, refusing to use applications which are insecure by
design is not
only better from a security standpoint but also tends to be
easier to use
because the users don't have to learn different, network-
dependent ways to
work.

I've been advocating the untrusted network approach for awhile but I can't claim the idea is particularly novel - of particular interest might be Abe Singer's 2003 report describing the San Diego Supercomputing Center's firewall-less network:

<http://www.usenix.org/publications/login/2003-12/pdfs/singer.pdf>

Re: Mac OS X Leopard firewall (Schmidt, [RISKS-24.89](#))

<Ted Lemon <Ted.Lemon@nominum.com>>

Fri, 2 Nov 2007 19:36:30 -0700

Look, I don't want to be an apologist for Mac OS X security, which I do not think is invulnerable. But this statement is kind of ridiculous. The idea that some networks are trustworthy and some aren't has been disproven time and time again over the past years. It's perfectly possible for a virus to be carried inside of a network and disseminate there, and it's happened and made news several times that I've noticed in the past couple of years. Imagine how many times it **didn't** make news, or was mentioned in passing in a story about botnets attacking from inside corporate networks, where the focus of the story, unbelievably, was not even **on** the idea that such a network had been penetrated by a virus infestation.

The problem here is not that Leopard trusts all networks equally -- that is appropriate, because no network is "trustworthy." The problem

is that Vista
lulls people into a false sense of security by suggesting that
it is only
when they are sitting in Starbucks that they are at risk of
attack. Nothing
could be further from the truth. If you examine all the
machines in all the
botnets in the world, the ones that were infected in Starbucks
don't amount
to a hill of beans...

✉ **Re: Plagiarism & technology (Re: Epstein, [RISKS-24.88](#))**

<"Bob Brown" <bbrown@spsu.edu>>

Sat, 3 Nov 2007 17:16:44 -0400

I am a college teacher and user of Turnitin.com. I've used it
for several
years for term papers, and occasionally for shorter papers. I
am very
familiar with what teachers see when they use this product or its
competitors.

> There are several problems with products of this sort:
> (1) False positives...

Turnitin.com and its various competitors do not detect
plagiarism; they
detect similarity of text in the student's paper to text found
elsewhere: on
the Web, in certain publications, and in previously-submitted
papers. The
teacher must then read the paper, checking for proper citation,
and where
appropriate, proper quotation. A teacher who does not do this
is both lazy
and intellectually dishonest.

It is perhaps unfortunate that Turnitin produces a "similarity score" that's expressed as a percentage of text that is similar to text found elsewhere because it can facilitate lazy and intellectually dishonest behavior by teachers. However, it does help teachers in detecting something that's bad, but not plagiarism: the cut-and-paste paper. In such a paper, everything is cited and quoted properly, it's just that none of it, with the possible exception of some glue sentences, was written by the student. The material went through the Windows clipboard and not through the student's mind; no learning took place. I tell my students that the cut-and-paste paper is not plagiarism, but neither is it evidence of learning, and the *best* grade such a paper can earn is a D-minus. (I also help them to write good papers by talking and writing about the process.)

> (2) Copyright infringement...

Bogus argument. Does the student who solves a series of math problems assigned by the teacher hold copyright in the answers? Of course not! I assign short ethics cases and the students write answers. That's more complicated because there is both a right answer and the expression of it. I'd argue that the student who gets the right answer has exhibited evidence of learning, but has not done creative work. In the case of a term paper or creative writing assignment, the student has (we hope) done some creative work, but it is generally work that would never have been done but for the assignment. It is a work made for hire, and the payment is

evaluation by
the teacher and a grade.

Further, Turnitin.com never "publishes" the papers that are uploaded, and publication is of the essence of copyright infringement. Teacher and student get to see the analysis, but no one else does. The only way to get to see what's in such a paper is to submit later a paper that is, at least in part, substantially identical. Those parts that are identical are called out, but what is highlighted is material in the *newly submitted* paper, not material in the stored paper. Turnitin.com does provide contact information for the teacher whose student submitted the original paper, and that teacher may then possibly release a copy if allowed by the school's policies and procedures.

I have not yet had a student object to using Turnitin.com on intellectual property grounds. If ever I do, I will ask how much money the student expects to make from the sale of the paper and whether the student would want a third party to earn a good grade by submitting a copy of the student's paper as his own.

(I am aware of the court cases. A Pennsylvania court decided that caller ID was an illegal wiretap, too. This issue is not yet decided, at least in the United States.)

The real value of a service like Turnitin is not in detecting plagiarism. I can do that better than any computer system I've seen so far because I know

my students' intellectual capacities and writing styles. I have, in fact, detected plagiarism not detected by Turnitin.com.

The real value is in plagiarism prevention. Students do not believe that I can detect writing that's not their own. They do, however, believe that "the computer" can detect similarity with text on the Web, and the student who is tempted, but knows the paper will be submitted to Turnitin.com, is more likely to make a good decision than a bad one. While I have not done a controlled study, I have observed fewer instances of plagiarism when Turnitin.com is used in a class than when it is not, and *that* is what's valuable.

Re: "Same ol' same ol'" ([RISKS-24.88](#))

<Eric Ball <eball@ca.ibm.com>>
Mon, 5 Nov 2007 13:13:27 -0500

I received a similar e-mail from my wife's credit card company. In that case the links didn't match the URLs because they went through the CC's 3rd-party marketing firm. I called the CC company and said they either had lousy security or incompetent marketing, and that I would cancel the CC if I received a similar e-mail. The CC has now been canceled for that reason.

✶ Re: Leaping onward

<Rob Seaman <seaman@noao.edu>>

Tue, 6 Nov 2007 16:31:43 -0700

Tony Finch opines:

The obvious answer is to leave UTC alone, even when it is an hour or more away from GMT. If the discrepancy becomes inconvenient for civil purposes then local time offsets can be adjusted. Local time changes do not need to be agreed globally and they do not need to be applied simultaneously around the world. Therefore no new mechanism or policy is needed to cope with a continuous UTC.

Rob Seaman responds:

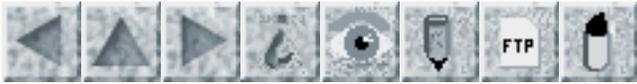
A brief (negative) response is to consider that computer scientists have raised all this ruckus over the need to track a single list of historical leap-second events. However, leaving the question to local officials replaces that single list with hundreds, or potentially thousands, of such lists that our software systems would need to consult.

Further discussion ensued and has been redirected to LEAPSECS:

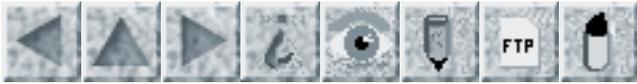
<http://six.pairlist.net/mailman/listinfo/leapsecs>

Seaman also notes:

Also see <http://www.physorg.com/news113282110.html>. The disruptions caused by unexpected Daylight Saving Time style jumps may not be the best model for establishing safe civil timekeeping practices.



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 91

Monday 19 November 2007

Contents

- [Reported impending asteroid was actually Rosetta](#)
[Paul Saffo](#)
- [Ship collision with San Francisco Bay Bridge](#)
[PGN](#)
- [Village auto crashes blamed on sat nav](#)
[Amos Shapir](#)
- [Is Car Safety Technology Replacing Common Sense?](#)
[Florian Liekweg](#)
- [Adi Shamir's bug attack](#)
[Jean-Jacques Quisquater](#)
- [Timing Glitch Affected Thousands in NYC Marathon](#)
[Henry Baker](#)
- [Hamilton Township election result flipped: programming error](#)
[PGN](#)
- [Cardinal sin? Scoreboard message](#)
[PGN](#)
- [The dangers of machine translation](#)
[Shoshannah Forbes](#)

- [Security company e-mail undercuts user education](#)
[Rex Sanders](#)
 - [Dangerous Mix of Globalization and Software](#)
[Stephen Smoliar via PGN](#)
 - [Re: Best practices to redact account numbers](#)
[Mark Seecof](#)
 - [Verizon phones make an audible alarm when 911 is dialed](#)
[Alex Burr](#)
 - [ACSAC 2007](#)
[Cristina Serban](#)
 - [ICRAT - Air Transportation Research Symposium](#)
[Dres Zellweger](#)
 - [REVIEW: "Network Security Hacks", Andrew Lockart](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Reported impending asteroid was actually Rosetta

<Paul Saffo <paul@saffo.com>>

Wed, 14 Nov 2007 14:37:21 -0800

[Incoming stone was actually Rosetta stone? PGN]

To make a long story short,

The Minor Planet Center, the world clearinghouse for information about

newly discovered asteroids, raised the alarm last week to track a

threatening celestial body. This would be one of the closest approaches

ever by a sizable asteroid -- its distance away being less than half the

diameter of the Earth. They announced that a previously unknown asteroid

would miss the Earth by just 5,600 kilometers. Then Denis Denisenko, of

Moscow's Space Research Institute (IKI), made an interesting discovery. He noticed that the incoming asteroid's track matched that of the European space probe Rosetta on a scheduled flyby of Earth. The Rosetta craft was launched from Europe's Guiana Space Center in early March of 2004; the purpose of the space probe is to place itself in low orbit around the comet Churyumov-Gerasimenko at a distance of 675 million kilometers from the sun. To get there, the billion-dollar craft will spend ten years boosting its velocity (using the gravity assist technique) with no fewer than three flybys of Earth and one of Mars. [Source: Bill Christensen, Near-Miss Asteroid Found to be Artificial, 12 Nov 2007; PGN-ed. Bill was reminded of Arthur C. Clarke's Rendezvous with Rama.] <http://www.space.com/business/technology/071112-technov-asteroid-mistake.html>

[Mark Brader noted a BBC item:

<http://news.bbc.co.uk/1/hi/sci/tech/7093402.stm>

and *The Register* did an amusing take:

"Muscovite skywatcher Denis Denisenko revealed that the menacing meteor

was in fact [STRUCK THROUGH: a European Union space battleship bent on

world domination] the European Space Agency Rosetta probe, passing close

to Earth for a long-planned gravity-assist "slingshot" manoeuvre.]

http://www.theregister.co.uk/2007/11/13/rosetta_asteroid_spacecraft_patrick_moore_cockup/

✈ Ship collision with San Francisco Bay Bridge

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

Mon, 19 Nov 2007 9:57:01 PST

[Despite many reports calling it a tanker,] The Cosco Busan was actually a container ship, and the fuel on board was solely for the purpose of running the ship.

<http://gcaptain.com/maritime/blog/ship-types-101-san-francisco-bay-bridge-oil-tanker-collision/>

The Coast Guard blames the pilot and the captain, and notes that its radar

resolution was inadequate to detect the impending collision.

<http://www.latimes.com/news/local/la-me-spill16nov16-ap,0,2939939.story>

Other reports of the 7 Nov 2007 incident indicate that some of the ship's

sensors malfunctioned, the GPS was misinterpreted by the captain, and the

pilot believed the captain rather than a radio warning.

⚡ Village auto crashes blamed on sat nav

<Amos Shapir <amos083@hotmail.com>>

Sun, 11 Nov 2007 17:45:57 +0200

This article from the BBC news site is about a small village in Wales which

had seen a sudden increase of heavy traffic through its narrow streets,

causing a lot of damage. Quote: "Residents were convinced that satellite

navigation was to blame for the damage".

It has become so bad that "In August, the Vale of Glamorgan council became so concerned over lorries being sent along narrow roads near St Hilary, it began trials of a sign warning drivers to ignore sat-nav directions."

Read the full story at: http://news.bbc.co.uk/1/hi/wales/south_west/7088105.stm

✦ Is Car Safety Technology Replacing Common Sense?

<"Dr. Florian Liekweg" <liekweg@ipd.info.uni-karlsruhe.de>>

Thu, 08 Nov 2007 19:38:58 +0100

<http://blog.wired.com/cars/2007/11/is-safety-techn.html>

In this blog post on the autopia blog, filed under "Safety" no less, Matthew Phenix reports his experience with a Volvo S80, focusing on the wide array of electronic "safety devices". He generalizes his impression with these devices - those of the S80 and others - with the words

"Do I feel safer knowing other drivers' cars are doing the things -- like checking mirrors and applying enough pressure to the brake pedal -- they should be doing themselves? Not really."

I couldn't agree more to this statement.

After the recent reports about GPS/SatNav-related issues ([RISKS-24.66](#),

"Another sat-nav accident: car destroyed, driver escapes", [RISKS-24.65](#),

"Don't let your navigation system fool you" and many others),

Phenix'
article covers a much broader area.

The Volvo "CWBS" has appeared in [RISKS-24.33](#) ("Volvo's self
braking car").

✶ Adi Shamir's bug attack

<Jean-Jacques Quisquater <jjqnews@quisquater.org>>
Fri, 16 Nov 2007 13:15:06 +0100

[http://www.nytimes.com/2007/11/17/technology/17code.html?
em&ex=1195448400&en=729de9307626c4e6&ei=5087%0A](http://www.nytimes.com/2007/11/17/technology/17code.html?em&ex=1195448400&en=729de9307626c4e6&ei=5087%0A)

Very recently Adi Shamir sent the following announcement to few
friends
(reproduced here with full permission from Adi Shamir). One
(possibly
hidden and on purpose) bug in any high-level microprocessor as
used in any
modern configuration can possibly leak secret keys used by
Public-Key
Infrastructures (PKI). Be careful, there is a major risk. J-JQ

[This attack is noted by John Markoff, Adding Math to List of
Security

Threats: Electronic System Could Be at Risk, *The New York
Times*,

17 Nov 2007, National Edition B4. PGN]

- - - - -

Research Announcement: Microprocessor Bugs Can Be Security
Disasters

Adi Shamir, Computer Science Department,
The Weizmann Institute of Science, Israel

With the increasing word size and sophisticated optimizations of

multiplication units in modern microprocessors, it becomes increasingly likely that they contain some undetected bugs. This was demonstrated by the accidental discovery of the obscure Pentium division bug in the mid 1990's, and by the recent discovery of a multiplication bug in the Microsoft Excel program. In this note we show that if some intelligence organization discovers (or secretly plants) even one pair of integers a and b whose product is computed incorrectly (even in a single low order bit) by a popular microprocessor, then ANY key in ANY RSA-based security program running on ANY one of the millions of PC's that contain this microprocessor can be trivially broken with a single chosen message. A similar attack can be applied to any security scheme based on discrete logs modulo a prime, and to any security scheme based on elliptic curves (in which we can also exploit division bugs), and thus almost all the presently deployed public key schemes will become vulnerable to such an attack.

The new attack (which we call a "Bug Attack") is related to the notion of fault attacks discovered by Boneh, Demillo and Lipton in 1996, but seems to be much more dangerous in its implications. The original fault attack required physical possession of the computing device by the attacker, and the deliberate injection of a transient fault by operating this device in an unusual way (in a microwave oven, at high temperature, with high frequency clock, or with a sudden spike in the power supply). Such attacks are feasible against smart cards, but are much harder to carry out

against

PC's. In the new bug attack, the target PC can be located at a secure location half a world away, and the attacker has no way of influencing its operating environment in order to trigger a fault. In addition, millions of PC's can be attacked simultaneously, without having to manipulate the operating environment of each one of them individually.

We now describe the basic idea of the new attack. We assume that the RSA decryption (or signature generation) is using the Chinese Remainder Theorem (CRT) which speeds up the operation by a factor of 4 compared to naive implementations, that each multiplication of big numbers proceeds by breaking them into the largest words which can be handled by the native multiplier in that microprocessor (typically 32 or 64 bits), and that all pairs of such words from the two numbers will be multiplied in some order. Knowing the target's public key n , the attacker can easily compute a half size number c which is guaranteed to be between the two secret factors p and q of n . For example, a number c which is the square root of n (rounded to the nearest integer) always satisfies $p < c < q$, and any number close to c is also likely to satisfy this condition. The attacker now chooses a message m which is equal to c , except that two low order words in it are replaced by a and b , and submits this "poisoned input" to the target PC.

The first step in the CRT computation is to reduce the input m modulo p and q . Due to its choice, m will be randomized mod the smaller p , but remain

unchanged mod the larger q . The next step in RSA-CRT is always to square the reduced inputs mod p and q , respectively. Since a and b are unlikely to remain in the randomized value of $m \pmod{p}$, the computation mod p is likely to be correct. However, mod q the squaring operation will contain a step in which the word a is multiplied by the word b , and by our assumption the result will be incorrect in at least one bit. Assuming that the rest of the two computations mod p and q will be correct, the final result of the two exponentiations will be combined into a single output y which is likely to be correct mod p , but incorrect mod q . The attacker can then finish off his attack in the same way as the original fault attack, by computing the gcd of n with y^{e-m} , where e is the public exponent of the attacked RSA key. With very high probability, this gcd will be the secret factor p of n . This completely breaks the security of this key.

How easy is it to verify that such a single multiplication bug does not exist in a modern microprocessor, when its exact design is kept as a trade secret? There are 2^{128} pairs of inputs in a 64x64 bit multiplier, so we cannot try them all in an exhaustive search. Even if we assume that Intel had learned its lesson and meticulously verified the correctness of its multipliers, there are many smaller manufacturers of microprocessors who may be less careful with their design. In addition, the problem is not limited to microprocessors: Many cellular telephones are running RSA or elliptic curve computations on signal processors made by TI and others,

FPGA or ASIC

devices can embed in their design flawed multipliers from popular libraries of standard cell designs, and many security programs use optimized "bignum packages" written by others without being able to fully verify their correctness. As we have demonstrated in this note, even a single (innocent or intentional) bug in any one of these multipliers can lead to a huge security disaster, which can be secretly exploited in an essentially undetectable way by a sophisticated intelligence organization.

⚡ Timing Glitch Affected Thousands in NYC Marathon

<Henry Baker <hbaker1@pipeline.com>>

Thu, 08 Nov 2007 07:31:58 -0800

In this year's New York City Marathon on 4 Nov 2007, runners had chips in their shoes that were intended to record when they crossed the starting line and the finish line. This compensates those runners for the time it takes to reach the starting line. However, the electronic timing system failed to record 2,300 runners out of a field of more than 38,000. Because good results in the NY race would enable qualification for the Boston Marathon, surmounting this problem this was rather crucial to some of those runners. Fortunately for them, the Boston officials accepted the self-reported times recorded by the timers of those individuals and accepted by NY. The "technical problem" was caused by interference (unspecified)

that reportedly disrupted the system for about three minutes at the start on one of three starting areas. One woman's recorded time was indeed off by almost three minutes, which may have been just enough to let her qualify for Boston.

(The official results are supposed to be posted on 19 Nov.)

[Source:

Abigail Lorge, Timing Glitch Affected Thousands in Marathon, *The New York Times*, 8 Nov 2007; PGN-ed]

[Considering which weekend this was ("fall back"), I'm amazed that the

timing wasn't an *hour* off... HB]

Hamilton Township election result flipped: programming error

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

Mon, 19 Nov 2007 14:12:17 PST

On election day, 6 Nov 2007, the results were reportedly reversed in one race, for trustee, in Hamilton Township, Lawrence County, Ohio, as a result of "a programming error" in ES&S software. Because the final two candidates for the Ironton City Council race were within four votes of one another, that race was also being reevaluated. In Proctorville, the mayor's race had a single vote separating the leaders, and the council race had a tie for the second seat. In Symmes Valley, the fiscal office winner also had a one-vote margin. And so on. [Source: Mark Shaffer *The Ironton Tribune*, 8 Nov 2007; PGN-ed]

<http://www.irontribune.com/articles/2007/11/08/news/news170.txt>

[Of course one of the main problems with many current electronic voting machines is that recounting is not particularly meaningful if the votes are already incorrectly recorded, in the absence of a definitive independent audit trail. PGN]

⚡ Cardinal sin? Scoreboard message

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

Sat, 10 Nov 2007 7:57:54 PST

An Illinois woman (identified only as C.B.) is suing the St. Louis Cardinals (damages at least \$25K) for allowing a text message that falsely suggested her 17-year-old daughter (A.B.) has an "STD") (of course, implying a sexually transmitted disease, rather than a "standard!") to be posted on the Busch Stadium jumbotron during a game, apparently requested by a school classmate of A.B. "The lawsuit, filed Wednesday in St. Louis Circuit Court, claims the 17-year-old girl was so traumatized by the message last year during a class trip that she stayed out of school the rest of the semester and took her finals in a school office to avoid ridicule." More than 48,000 people attended the game. [Source: Lawsuit filed over text message on St. Louis Cardinals board, KMOV, 9 Nov 2007; PGN-ed]

It seems that anyone can text a cell-phone message and have it displayed, for a small fee. The expected uses are presumably proposing marriage, announcing an engagement, wishing happy birthday, and other similar occasions. However, this service clearly opens up all sorts of opportunities for misinformation, but also opportunities for intentionally having defamatory messages posted so that you can sue. Incidentally, KMOV reminded its viewers that at the first home game of 2006, a proscribed four-letter word appeared on the screen, which management attributed to a "technical error". The KMOV website has lots of further discussion.

✶ The dangers of machine translation

<"Shoshannah Forbes" <xslf@xslf.com>>

Tue, 13 Nov 2007 19:23:17 +0200

Sending out machine translation without reading the result resulted in a diplomatic incident:

<http://www.guardian.co.uk/g2/story/0,,2206335,00.html?gusrc=rss&feed=technology>

"So when indignant officials at the Dutch foreign ministry received an email from a group of Israeli journalists that began, "Helloh bud, enclosed five of the questions in honor of the foreign minister: The mother your visit in Israel is a sleep to the favor or to the bed your mind on the conflict are Israeli Palestinian," they might perhaps have guessed what had

happened.

Sadly, they did not."

The Guardian claims that the journalists used the popular translation engine Babelfish, but this appears to be incorrect. Babelfish doesn't handle Hebrew. Hebrew sources indicate that they may have used Babylon.

Shoshannah Forbes <http://www.xslf.com>

[Also noted by Mark Brader. PGN]

Security company e-mail undercuts user education

<Rex Sanders <rsanders@usgs.gov>>

Wed, 14 Nov 2007 12:42:54 -0800

We've seen many reports of financial institutions sending e-mail virtually indistinguishable from phishing and spam.

Lately, I've been in the market for new computer security hardware and software. Security companies seem to have taken email lessons from the worst financial institutions.

Some common problems in security company emails:

- * "Click here if your email program has trouble displaying this email"
- * Images and links that point to third party web sites.
- * Unsubscribe links that point to third party web sites

These security companies are undercutting user security education. We have a hard time keeping users from clicking on links in suspicious

emails; we
don't need security firms reinforcing bad behavior.

Rex Sanders, USGS <http://tinyurl.com/84kdo> :-)

⚡ **Dangerous Mix of Globalization and Software (Stephen Smoliar)**

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

Tue, 13 Nov 2007 14:20:38 PST

Stephen Smoliar's blog contains various items that might interest RISKS readers.

There is one rather egregious example of a spelling corrector:
<http://therehearsalstudio.blogspot.com/2007/04/dangerous-mix-of-globalization-and.html>

The most recent, today, considers some of the problems that the San Francisco Public Library is experiencing in its attempts to modernize:
<http://therehearsalstudio.blogspot.com/2007/11/speak-out-against-defective-technology.html>

⚡ **Re: Best practices to redact account numbers (Watson, [RISKS-24.82](#))**

<Mark Seecof <mseecof@jural.com>>

Fri, 16 Nov 2007 17:51:12 -0800

Tom Watson's message ([Risks 24.82](#)) about redacting account numbers attracted my attention (sorry I'm running behind).

Besides the risk associated with switching methods (access to old and new redacted numbers revealed complete number), there is a risk with choice of redaction schemes--and many knuckleheads are choosing wrongly nowadays.

Credit-card systems seem to provide cultural leadership in account-number hashing. The idea is to show people enough digits so they know which of their cards you want to refer to, but too few to let an observer guess the whole number. Four digits works well. By the birthday paradox, it's not likely you'll get collisions when customers have much less than 100 cards. Even the shortest credit-card numbers are 12 digits long. The first few digits identify the bank so they're easy to guess. The last digit is a checksum so it says something about the rest, but an adversary will still have to guess, say, four digits. Most cards have 15 or 16 digit numbers now, making you guess seven or eight digits; an adversary will likely guess someone else's number.

With (US) Social Security numbers and bank account numbers things are different. The last four digits of the SSN are the critical ones! The first five are easy to guess (they encode issuing location and date). People think that it's smart to ape the last-four-digits scheme used with credit-card numbers, but we don't show an SSN hash because people have multiple SSN's, we show it to help distinguish people with similar names. For that purpose the first few digits are adequate and much less

sensitive.

Bank account numbers present a similar problem. The first digits often identify branch and account type (I will pass over ABA check routing numbers which are trivial to guess) so the trailing digits are generally more sensitive. Most people need to see enough digits to tell which account out of several they have with one bank (checking/savings/etc.) is the subject of communication. For many banks, the best plan would be to show some leading digits from the account number--even though they'll be the same for many customers they'll be different for each account of any one customer.

It appears that someone at Watson's bank was aware of this years ago and set up the best system. Then (perhaps along with some other "upgrades") some dimwit decided that since it's good to show "last four digits" with credit cards, it must also be good to show the last four digits of checking account numbers. This kind of failure is why RISKS DIGEST will never lack for material!

⚡ Verizon phones make an audible alarm when 911 is dialed

<Alex Burr <ajb44.geo@yahoo.com>>
Sat, 10 Nov 2007 11:45:18 +0100

Just the thing for those hostage and robbery situations - I don't think:

<http://www.kvue.com/news/local/stories/110907kvueverizonalarm-bm.1f46e16ee.html>

"The alarm is not ear-splitting, but it is loud enough to be heard at least several yards away"

Verizon claims the FCC requires this. The FCC says it's not that stupid.

ACSAC 2007

<jay-kahn@att.net>

Sun, 18 Nov 2007 03:02:49 +0000

Twenty-Third Annual Computer Security Applications Conference
(ACSAC)

Practical Solutions To Real World Security Problems

December 10-14, 2007

Miami Beach Resort and Spa

Miami Beach, FL, USA

Cristina Serban, PhD, CISSP

2007 ACSAC Conference Chair

Hotel and Conference Registration at <http://www.acsac.org/>

[This message is unfortunately less timely than it ought to be. 19 Nov is

the deadline for early registration and the discounted hotel rate. PGN]

ICRAT - Air Transportation Research Symposium

<a.zellweger@comcast.net (Dres Zellweger)>

Wed, 14 Nov 2007 14:47:02 +0000

[Dres is a long-time RISKS contributor, educator, and former FAA Advanced Automation director. He has been relatively quiet in RISKS lately. PGN]

ICRAT 2008: Papers due 31 January, 2008 See www.ICRAT.org.
June 1-4, 2008 at George Mason University, Fairfax, VA

ICRAT is an excellent forum for young researchers within air transportation to share their work, expand their professional network, and gain new knowledge and inspiration. This third edition of ICRAT includes one day of tutorials, two days of technical presentations and a doctoral symposium where PhD students can expose their research problems to get advice from established scientists in the field. Parallel invited workshops on Single European Sky ATM Research and US NextGen initiatives are also expected.

ICRAT 2008 is jointly organized between EUROCONTROL Experimental Centre and George Mason University, and is sponsored by the US Federal Aviation Administration, NASA, the European Commission, and by EUROCONTROL. Financial support for participating in this conference is available to a limited number of young scientist and PhD students. We expect to be able to cover travel expenses, room and board for students from the U.S. whose papers are accepted.

REVIEW: "Network Security Hacks", Andrew Lockart

<Rob Slade <rMslade@shaw.ca>>

Thu, 08 Nov 2007 15:15:33 -0800

BKNTSCHK.RVW 20070921

"Network Security Hacks", Andrew Lockart, 2007, 0-596-52763-2,
U\$29.99/C\$38.99

%A Andrew Lockart

%C 103 Morris Street, Suite A, Sebastopol, CA 95472

%D 2007

%G 0-596-52763-2 978-0-596-52763-1

%I O'Reilly & Associates, Inc.

%O U\$29.99/C\$38.99 707-829-0515 fax: 707-829-0104 nuts@ora.com

%O <http://www.amazon.com/exec/obidos/ASIN/0596527632/>

[robsladesinterne](#)

<http://www.amazon.co.uk/exec/obidos/ASIN/0596527632/>

[robsladesinte-21](#)

%O <http://www.amazon.ca/exec/obidos/ASIN/0596527632/>

[robsladesin03-20](#)

%O Audience i Tech 2 Writing 1 (see revfaq.htm for explanation)

%P 298 p.

%T "Network Security Hacks, 2nd Edition"

Chapter one lists twenty-two tips for using a number of utilities and programs to enhance the security of UNIX systems. The explanations are clear and specific, although you would probably have to be really familiar with UNIX administration to get the full benefit of these suggestions.

Windows gets fourteen hacks in chapter two. While useful, these could have had more explanation in some cases, in regard to the limitations and

pitfalls of the recommendations. A variety of tools that address aspects of confidentiality are listed in chapter three. Almost all of the firewall

tools discussed in chapter four are for UNIX, although some do

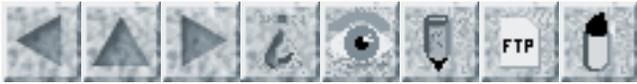
have Windows versions. (The Windows firewall is discussed, but so poorly that one almost suspects that the whole purpose is to force the reader to use the suggested alternative.) Advice on securing various services and applications (mostly from Guess What Operating System) is given in chapter five. Again, the bulk of the network security tools discussed in chapter six are for UNIX, with some Windows editions. The wireless tips, in chapter seven, work best with UNIX. The same is true with the logging tips in chapter eight, although there is mention of arranging to have Windows report to a syslogd. Network monitoring, and some analysis thereof, is in chapter nine. Tunnels and VPN (Virtual Private Network) products are detailed in chapter ten. Most of the network intrusion detection material in chapter eleven concerns Snort. (You are not my NIDS, you are a Snort!) Chapter twelve lists a few recovery and response tools.

If you run a UNIX system and network, this book enumerates many useful tasks, settings, and tools that will help to make your systems and network more secure.

copyright Robert M. Slade, 2004, 2007 BKNTSCHK.RVW 20070921
rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<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

Search RISKS using [swish-e](#)

Volume 24: Issue 92

Monday 17 December 2007

Contents

- [Private details of EVERY family in Britain 'lost' by taxman in major security gaffe](#)
[Peter Houppermans](#)
- [UK Government disks were not well encrypted](#)
[Peter Houppermans](#)
- [Whole of UK Child Benefit records on CD lost in the post](#)
[Peter Mellor](#)
- [Bad Health Informatics Can Kill](#)
[Brian Randell](#)
- [Space Shuttle Year End Rollover problem](#)
[Jan Wolitzky](#)
- [Lost in Translation: Rail Signal Consistency + Questionable Reporting](#)
[Chuck Weinstock](#)
- [Computer Security Meets Alcohol Breath Testing](#)
[Eric Van Buskirk](#)
- [Miss California? Sensible vote counting did!](#)
[Peter G. Neumann](#)
- [Daylight savings switch causes twins paradox](#)
[Tony Luck](#)

- [Risks: Computer Glitch Leads To Kmart Brawl](#)
[Gabe Goldberg](#)
 - [DSL outage hits some AT&T customers](#)
[Yahoo! News via Stephen W Smoliar](#)
 - [Drunk a better guide than sat nav](#)
[Dan Jacobson](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Private details of EVERY family in Britain 'lost' by taxman in major

<Peter Houppermans <peter@houppermans.com>>

Tue, 20 Nov 2007 19:06:57 +0100

security gaffe

The Chancellor was rocked by a new crisis this evening over the loss of confidential bank details of virtually every family in Britain.

Alistair Darling had to make an emergency statement to the Commons revealing that records of 7.2 million bank accounts of all parents or guardians who claim child benefits had gone missing.

MPs gasped when he revealed that the names, addresses, bank numbers and National Insurance numbers of all those affected had been on two computer discs which had been lost.

A total of 25 million people's names are on the discs, potentially leaving them all at risk of identity fraud. Britain's most senior taxman, Paul Gray, quit his 170,000-pound--a-year job as head of HM Customs and Revenue in the wake of the Treasury blunder.

<<http://tinyurl.com/2ubzzm>>, full URL

<http://www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=495188&in_page_id=1770&in_page_id=1770>

At present it appears the information was at least encrypted, but it defies belief that data of such sensitive nature was despatched in this form without being accompanied with the most basic form of tracking. Plus ca change.

UK Government disks were not well encrypted

<Peter Houppermans <peter@houppermans.com>>

Wed, 21 Nov 2007 09:12:11 +0100

According to more recent reports, the extreme blunder made by the UK "HM Revenue and Customs" by sending two CDs with the personal details of approx 25 million people per unsecured courier is worse than first reported.

Later news reports suggest that the original story of this data being at least "encrypted" may be inaccurate, or may be a bit of an overstatement when it comes to the kind of encryption used (ROT 13, maybe?).

http://uk.news.yahoo.com/pressass/20071121/tuk-astonishment-over-information-error-6323e80_1.html

This is an absolutely unbelievable blunder, especially given the sensitivity of the data. In addition, there are electronic connections on multiple security levels between those departments - there was really no

need at all
for that data to travel physically. And this lot wants the
population to
agree to a central IDcard scheme?

🚀 Whole of UK Child Benefit records on CD lost in the post

<MellorPeter@aol.com>

Thu, 22 Nov 2007 08:54:54 EST

Two CD-ROMs containing the entire Child Benefit database held by Her Majesty's Revenue and Customs (HMRC) have gone missing in transit from the HMRC Child Benefit Office in Washington, Tyne and Wear, to the National Audit Office (NAO) in London.

The information here is mostly a summary of pages of the BBC's site:

http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm

http://news.bbc.co.uk/1/hi/uk_politics/7106366.stm

http://news.bbc.co.uk/1/hi/uk_politics/7104368.stm

... updated from BBC Radio bulletins of 21st and 22nd November.

Information from commentators to The Register is also interesting:

http://www.theregister.co.uk/2007/11/21/reader_comments_on_hmrc/page2.html

The New York Times covered the story on 22nd November:

<http://www.nytimes.com/2007/11/22/world/europe/22data.html?th&emc=th>

For non-UK readers, the Child Benefit is a fixed payment to parents, (normally the mother) of every child in the UK under 16, and to older

children in full-time education. It is taken up by almost 100% of those eligible. Amounts: 18.10 pounds a week for the first child; 12.10 pounds a week for further children. (\$36.30 for the first child; \$25 per additional child - NYT) Payments are administered by HMRC.

The NAO is the UK watchdog body on public expenditure, and needed to know the amounts paid in Child Benefit, as part of its normal work.

The following was the sequence of events (adapted from the BBC report):

MARCH 2007

The head of NAO requested from the manager of Child Benefit a copy of the Child Benefit records for the whole of the UK. Only financial information was needed. The request made it clear that personal details could be removed, to "de-sensitize" the data.

The manager of Child Benefit e-mailed the head of NAO to say that de-sensitizing the data could not be done for reasons of cost, and that the complete data would be sent. This message was copied to one of the directors of HMRC.

A "junior official" at HM Revenue and Customs sent to the NAO a full copy of HMRC's child benefit data. That information was later safely returned.

18 OCTOBER

Child benefit data was again sent to the NAO by a "junior official", using the courier company TNT, which operates the HMRC's internal mail system.

The package contained two CDs, containing details of 25 million individuals.

It has been reported that the data was password protected but not encrypted.

The package was not recorded or registered, and failed to arrive. (The repeated statements that the package was "not recorded or registered" are puzzling. See my comment below.)

24 OCTOBER

The NAO told HMRC it had not received the package. An HMRC spokeswoman said the official believed it may have been delayed by the postal strikes or in the NAO's office move and did not report it. A second copy was sent by registered post and arrived safely.

8 NOVEMBER

Senior HMRC management were informed that the 18 October package was missing.

10 NOVEMBER

The Chancellor, Alistair Darling, was informed and told Prime Minister Gordon Brown. Mr Darling ordered an immediate investigation and searches of all premises where the package might be, as well as action to ensure it does not happen again.

12 NOVEMBER

Mr Darling was told by HMRC that evidence has been found which might help to find the missing package (as stated on the BBC web site: there has been no public statement about what this "evidence" might have been).

14 NOVEMBER

The chancellor decided the HMRC searches had failed and told HMRC chairman Paul Gray to call in the Metropolitan Police.

15 NOVEMBER

The chancellor went to Information Commissioner Richard Thomas, who agreed that remedial action must be taken before a public statement is made.

(Keeping Joe Public and his missus informed is the lowest priority, as usual!)

12-18 NOVEMBER

Mr Gray told Mr Darling he felt he should resign (i.e., Mr Gray, not the Chancellor!). The Chancellor sought the advice of the Financial Services Authority and Serious Organised Crime Agency, while banks were alerted by HMRC.

20 NOVEMBER

Mr Gray resigned following an announcement that Mr Darling was to make a statement to the House of Commons. The chancellor outlined what had happened and announced an investigation of HMRC's security procedures by PricewaterhouseCoopers chairman Kieran Poynter, alongside the Independent Police Complaints Commission, which monitors the HMRC.

- - - -

Some interesting points arise from this comedy of errors:

We have been continually told that the posting of the CDs was done by a "junior official" who was acting "in breach of security procedures", and a

23-year-old civil servant has duly resigned.

It was speculated that he might have been a temporary, but it has now come to light that he was a permanent member of staff. As such, he should have known the "security procedures", whatever these were. Also, as a civil servant, he would have been subject to the Official Secrets Act.

Several serving or retired civil servants have made interesting comments to The Register (see URL above) about this "junior" official. For security reasons, a junior would not have had a CD burner as part of his office workstation. The active co-operation, as well as authorisation, of his manager would therefore have been required.

Also for security reasons, he would not have had a personal e-mail address at the office. There is, in any case, a 4Mb size limit to e-mail attachments, which would preclude electronic transmission (encrypted or otherwise) and was presumably the reason for sending CDs by snail-mail. One informed guess is that what was sent was a .mdb file, zipped using a password.

The junior official was therefore following his manager's explicit instructions, and using a procedure which had become routine. His responsibility should have ended at the point when he dropped the package into the internal mail, but he became a convenient scape-goat when the procedure failed, as it would sooner or later.

However, that was before the existence and contents of the e-mail from the

head of Child Benefit Office to the head of NAO were made public on the 21st November. (It seems that it was leaked to the Conservative Party, who were not slow to use it as a rod with which to beat the government.) The fact that it was cc'd to a director of HMRC means that the top brass were fully aware that unencrypted personal data for half the people in the UK were routinely being shipped on CD by an insecure route.

The contention that de-sensitizing the data would have been too expensive does not bear scrutiny. If all that was needed was to delete names, addresses and NI numbers, then this amounts to deleting some columns from a relational database. which is a few minutes' work. However, it is likely that the NI number would be at least a part of the primary key, so that it could not be removed without compromising the integrity of the data. It would have been necessary to have replaced it with another unique but arbitrary identifier. Also, the NAO might have required at least the first part of the post code in order to break down payments by region. All of this is pure speculation, of course.

Regarding the peculiar statement that the package was "not recorded or registered":

"Recorded delivery" and "Registered mail" are special services provided by the UK Post Office, and mean that, for a charge, one can ensure that a valuable package obtains VIP treatment or that its movements can be fully traced, which is not the case with normal postal delivery. I

use it if, for example, I need to send my birth certificate somewhere for an official purpose.

One would expect a courier to "record and register" every item entrusted to its care. (If I buy a pair of socks over the internet, I have to sign for it when the man in the van turns up on my doorstep.) TNT would (surely?) have signed in and out *every* package that they shipped, and must have been able to demonstrate basic competence in doing this in order to get the contract for handling HMRC's internal mail.

Regarding the possibilities of fraud:

The data includes: National insurance (NI) number Name, address and birth date Partner's details Names, sex and age of children Bank/savings account details ... quite useful for an identity fraudster, particularly the NI number. There is plenty of scope here for a fraudster to redirect payments.

We have been told by the Chancellor and Prime Minister that there is no evidence that the data has fallen into the "wrong hands", but since no-one knows whose hands it is in (if anyone's: it might be lying in the back of a van) this is just the usual reassuring bull***t from the government.

In two separate incidents in September, records of about 15,000 people's details went missing after being sent by HMRC to Standard Life Insurance, and a laptop containing around 400 ISA (individual savings accounts)

customers' details was stolen. (HMRC deals with tax as well as benefits.)

Government data security is now a **very** hot political potato.

Paul Gray has at least had the decency to resign. Whether his head will

placate the mob remains to be seen. In the meantime, the allegations that

the government could not guarantee adequate security for the data to be held

for the proposed national Identity Card scheme have gained new force.

Peter Mellor; Mobile: 07914 045072; email: MellorPeter@aol.com

Telephone and Fax: +44 (0)20 8459 7669

Bad Health Informatics Can Kill

<Brian Randell <Brian.Randell@ncl.ac.uk>>

Mon, 10 Dec 2007 22:30:56 +0000

I've just come across the document

Bad Health Informatics Can Kill

from the Working Group for Assessment of Health Information Systems of the

European Federation for Medical Informatics (EFMI)

"ICT can have positive impact on health care, but there are also examples on

negative impact of ICT on efficiency and even outcome quality of patient

care. Medical informaticians should feel responsible for the effects of ICT

on patients and public. Systematic analysis of ICT errors and failures is

the precondition to be able to learn from negative examples and to design

better health information systems. This document contains summaries of a number of reported incidents in healthcare where ICT was the cause or a significant factor. For each incident or problem at least one link to a source will be provided. With the following list, we want to raise awareness on this important issue, and provide information for further reading"

Full document at:

<http://iig.umat.ac.uk/efmi/badinformatics.htm>

School of Computing Science, Newcastle University, Newcastle upon Tyne,
NE1 7RU, UK +44 191 222 7923 <http://www.cs.ncl.ac.uk/~brian.randell/>

Space Shuttle Year End Rollover problem

<Jan Wolitzky <jwolit@optonline.net>>

Sun, 09 Dec 2007 17:39:01 -0500

NASA has been flying the Space Shuttle for more than a quarter century without ever having a mission in space over New Year's Eve, because its computer software could not be trusted to behave correctly when the Julian date rolled over from 365 or 366 to zero. Earlier this year, NASA announced that it had finally fixed the Year End Rollover (YERO) problem (<<http://www.nasaspaceflight.com/content/?cid=5026>>).

When they scrubbed today's STS-122 Atlantis launch attempt because of problems with the engine cut-off fuel sensors, NASA set the next

try for no
earlier than January 2, 2008, in part (reportedly) because of
YERO software
concerns.

It appears that NASA doesn't have a great deal of confidence in
their date
problem fix. Does anyone have details of where this issue
stands now?

✈ Lost in Translation: Rail Signal Consistency + Questionable Reporting

<Chuck Weinstock <weinstock@sei.cmu.edu>>

Wed, 5 Dec 2007 19:36:52 -0500

On 30 Nov 2007 an Amtrak passenger train approaching Chicago's
Union Station
slammed into the rear of a freight train occupying the same
track. Speed
recorders showed that the train was doing 40mph when the
engineer went into
emergency about 9 seconds before the crash. The signal on the
line, operated
by Norfolk Southern, was set so that the train should have been
going 15mph,
prepared to stop.

According to an article in the 4 Dec 2007 edition of the
Chicago Tribune

http://www.chicagotribune.com/news/local/chi-traincrash_04dec04,0,6705498.story

a cause of the accident may have been a combination of the
engineer's
relative inexperience and the surprising (to me) fact that the
same signal
indication on different railroads may mean different things.
According to

the Tribune: "The system of color-coded signals evolved over the last century or more, and the operating rules that govern them were created independently, based on the need of individual railroads."

The NS signal was showing red-over-yellow which, on that railroad signifies the 15mph restriction. The Amtrak train in question began it's journey from Grand Rapids, MI to Chicago on a different railroad where the red-over-yellow indication can mean something else.

Also from the article:

"An engineer's job these days is a lot more difficult than people realize," said Chip Pew, a safety specialist in the rail division of the Illinois Commerce Commission.

"Envision something as simple as a stop sign to mean as many as four different things depending on what railroad territory and what state you are in," Pew said. "We need to consider at least some national operating rules so red over yellow means red over yellow everywhere to eliminate the possibility of misinterpretation."

Not from the article: according to a friend who is knowledgeable about railroad signaling systems says that red-over-yellow always means some form of "slow down stupid" even if not exactly the same form on each railroad.

Computer Security Meets Alcohol Breath Testing

<Eric Van Buskirk <swiver@cox.net>>

Mon, 3 Dec 2007 21:23:55 -0700

Recent developments in DUI litigation unexpectedly bleed into the realm of computer security.

INTRODUCTION

Computer security enthusiasts are naturally interested in software quality.

They know that proper software engineering and development is necessary for the justified extension of trust to computing and communication systems.

The search for trust appears to have lately received an unexpected ally:

according to a small but growing number of DUI defendants, breath alcohol

testing devices cannot be trusted unless defense experts are permitted to

analyze the source code for the software that controls them.

Is there now an alliance between DUI defendants and computer security

professionals? To the extent that they are both interested in trust of

computing services, the answer is, "yes."

The search for trust is really a search for dependability.

Dependability is

an umbrella concept in computer science that includes five core components:

integrity, availability, safety, maintainability and reliability.¹ Those

who pursue computer security recognize the first two components as

essential. Those who use evidence that is i) scientific or technical, and

ii) the output of a computer should recognize the last as critical.² Thus,

DUI defense and computer security are indeed joined by their

respective
pursuits of computer dependability and trust.

However, this alliance is certainly not to the exclusion of police, crime labs, and prosecutors. To the extent evidence is the output of a computer, such as a breath test device, law enforcement pursues computer dependability with zeal equal to (probably exceeding) that of the defense.

Law enforcement pursues the reliability of breath test evidence using a range of elaborate methods. Central to those methods is black box testing.

In this context, black box testing involves the input of certified known solutions of ethanol into a breath testing instrument. The idea is that, if the instrument measures the known inputs correctly both before and after the defendant's tests, then by implication the instrument must be working properly and accurately at the time of the defendant's tests. At trial, prosecutors depend, in part, on this "before/after" testing to persuade judges and juries that evidence from a given breath testing instrument is reliable and trustworthy.

Some DUI defendants are recently claiming that this black box testing is insufficient to establish the reliability of breath test evidence. One notable example is the case of State v. Chun, a consolidated case involving 20 defendants who collectively demanded that the State of New Jersey (hereinafter, "State") disclose the source code for its breath testing instrument, the Draeger brand Alcotest 7110 MKIII-C.3 The Chun defendants

alleged that the reliability of the State's breath test evidence could only be established by a post-hoc source code review or audit. In particular, they claimed that "an actual source code review is necessary as there could be hidden techniques [in the software] that would allow for altering data and/or blatant coding errors that skew the accuracy of the instrument's results."4 If permitted, a post-hoc source code review would be quite a commitment, since the firmware for the Alcotest breath tester contained more than 45,000 lines of C/C++ code.

After protracted litigation, the Chun defendants convinced a court to grant review of the Draeger Alcotest source code firmware, version NJ3.11 (the actual version at issue in New Jersey). So that the defense was not left with the first, last, and only word on the "quality" of the NJ3.11 firmware, Draeger also contracted an expert to conduct a source code review. Finally, to resolve anticipated differences and to facilitate understanding, the court appointed its own expert to report on the work of the parties' experts.

THE CHUN SOURCE CODE REVIEWS

The defense hired Base One Technologies to conduct a static source code review. Base One used the following tools to conduct its review: Lint, MS Visual C++ Development Environment and Compiler, Borland C++, IAR Embedded C Compiler, Understand C code analyzer, Source Format X, Beyond Compare, and others. Since at least some of the comments for the NJ3.11

source code were in German, Base One used AltaVista Babelfish web translation service to translate the comments into English.⁵

In its final report, Base One made a number of criticisms of the NJ3.11 firmware.⁶ Perhaps the most incendiary charge, and the one most quoted on DUI defense attorney blogs, was that, in some cases, if a diagnostic routine fails, then the Alcotest "will substitute arbitrary canned data values" thereby affecting the breath measurements. The apparent implication of this allegation is that the Alcotest (at least for version NJ3.11) fabricates breath test evidence.

Base One made other notable findings. It said there was "proof of incomplete testing" of the code. This is an odd observation to make since it is well established that complete testing of non-trivial software is "impossible."⁷ Base One also wrote that "catastrophic error detection" was improperly disabled; that the firmware would not pass "U.S. industry standards" for software and testing; that the programming "does not insulate/protect modules or data"; and that "incorrectly coded or modified functions can inadvertently modify a data value not part of that routine's sphere of influence."

Prior to submission to the Chun court, Base One's report was assessed by the court's source code expert, the CMX Group.⁸ CMX was mostly critical of Base One's report. In particular, CMX wrote that more than a few of Base One's

claims were "unsupported," or contained "misleading observations," or were "pure speculation," or had no supporting evidence, or were flatly contradictory. CMX also impugned Base One's knowledge of software standards as being "inaccurate." Further, CMX said that Base One used inappropriate "innuendo" as well as unsubstantiated phrases such as "clearly" and "ample evidence," and also used non-specific phrases such as "industry standards" without sufficient elaboration. Finally, CMX found as empirically unsupported Base One's claim that the NJ3.11 firmware substitutes arbitrary data values for authentic ones.

CMX also wrote that the Base One reviewer may be "unaware" of some system testing tools necessary to perform an adequate review, or may not have had much experience in the relevant technologies. CMX noted that Base One's unspecific, misdirected, or false statements demonstrated "why companies do not want to expose their internal code.[since] [i]t looks as if they are covering up error while, in reality, this is the way that all code has to be written for controlling and coordinating hardware." In sum, CMX concluded Base One "[did] not succeed" in dislodging the presumption of reliability of the Alcotest 7110 MKIII-C breath testing device, firmware version NJ3.11.9

For its part, Alcotest manufacturer Draeger hired SysTest Labs, a nationally known software testing company, to review of the NJ3.11 firmware. SysTest conducted a line-by-line, static code review, but did not stop there: it also performed code tracing, reverse engineering, code

navigation and code metrics. SysTest used Understand C, Fortify SCA, and in-house software assessment tools. Instead of using Babelfish, SysTest employed a professional, human translation service to interpret the German source code comments. SysTest documented 602 hours of labor on its source code review.

SysTest also found problems with the NJ3.11 code. It noted that critical test data was stored in global variables, a practice that is undesirable "because any function in the application can [theoretically] change the data." SysTest noted at least 56 uncalled functions, at least as many documented uncalled objects, one documented unused type, numerous functions with higher than recommended "cyclomatic complexity," 10 non-descriptive variable names such as "dummy" and "temp," and a buffer overflow. However, in spite of the problems found, SysTest concluded that none affected the reliability of the NJ3.11 firmware breath tests.

As opposed to assessment of Base One, the Chun court's expert (CMX) wrote favorably of SysTest's review. CMX found almost all of SysTest's claims were "substantiated," and that its analysis was "impressive" in that it were not only able to run both "code stylistic" tests, through the use of automation tools, (as Base One did) but also a series of logical tests of the application by submitting combinations and permutations of data that would expose the potential buffer overflow condition. CMX also noted that, "[i]n contrast to the Base One Technologies review, the SysTest Labs report

is replete with empirical listings and line counts of examples of the conditions, and criticisms they found."

CONCLUSION

The facts in Chun presented an enormous opportunity to advance the cause of dependable computing. Were the defense able to raise legitimate reliability issues regarding the NJ3.11 firmware, it is likely that the issue of dependable computing would have received increased attention, understanding and respect from the public at large.

Unfortunately, however, the defense flubbed this important opportunity.

Interested readers who take the time to read the Chun litigation material

will likely conclude that the defense accomplished very little with its

source code review. Base One's review was contradictory, undocumented,

non-empirical, misleading, and speculative. And although the SysTest report

was mostly supportive, some will undoubtedly question whether 602 hours of

post-hoc analysis, by a manufacturer-contracted expert, is sufficient to

guarantee the reliability of NJ3.11 code. Consequently, computer security

enthusiasts and genuine dependable computing advocates shall continue to

wait for the untutored establishment to understand and to appreciate the

importance of proper software quality assurance.

1 Avizienis, et al. "Basic Concepts and Taxonomy of Dependable and Secure

Computing," IEEE Transactions on Dependable and Secure Computing, Vol. 1,

No. 1, at 13, January March 2004.

- 2 Kumho Tire Co. v. Carmichael, 526 U.S. 137 (1999).
- 3 Supreme Court of New Jersey, Docket No. 58-879, available at http://www.risk-averse.com/index_files/chun.pdf.
- 4 Norman Dee, CMX Group "Comments on the Source Code Reviews," available at http://www.risk-averse.com/index_files/sm.pdf.
- 5 John J. Wisniewski, Base One Technologies, "Report on Behalf of the Defendants," available at http://www.risk-averse.com/index_files/bo.pdf.
- 6 Id.
- 7 Kem Caner, "The Impossibility of Complete Testing," SOFTWARE QA, v.4, #4, p. 28 (1997), available at <http://www.kaner.com/pdfs/imposs.pdf>.
- 8 Supra note 3.
- 9 Supra note 3.
- 10 In its report, SysTest defined "cyclomatic complexity" as a "standard measure of source code complexity indicative of both understandability and maintainability." See SysTest, "Assessment Report for Draeger Safety Diagnostics, Inc.," available at http://www.risk-averse.com/index_files/st.pdf.

Eric Van Buskirk, JD, MA, CISSP

🔥 Miss California? Sensible vote counting did!

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

Tue, 4 Dec 2007 11:23:12 PST

A human accounting mix-up led to the wrong woman being crowned Miss California USA. Apparently lowest points were given to the winner and highest points to the fourth runner-up. Christina Silva, 24,

was declared
the winner of the annual state beauty pageant, but after the
error was
detected, she gave up the title to Raquel Beezley, who was
originally named
the second runner-up. New Miss California Named After Error,
The Huffington
Post, 3 Dec 2007 [PGN-ed]

<http://www.huffingtonpost.com/huff-wires/20071203/odd-miss-california>

Miss California USA: <http://misscaliforniausa.com>

⚡ Daylight savings switch causes twins paradox

<"Luck, Tony" <tony.luck@intel.com>>
Tue, 20 Nov 2007 10:36:04 -0800

Peter is Allison's older brother because he was born 34 minutes before her.
Yet his birth certificate says 1:32AM on November 4th, while his sister's birth certificate says 1:06AM making her apparently 26 minutes his senior.

<http://www.wral.com/news/local/story/2011296/>

⚡ Risks: Computer Glitch Leads To Kmart Brawl

<Gabe Goldberg <gabe@gabegold.com>>
Tue, 27 Nov 2007 15:56:47 -0500

Computer Glitch Leads To Kmart Brawl; 2 People Arrested

The store was running a promotion to give away \$10 to anyone

applying for
its credit card, but the computer glitch led to everyone's
application being
approved, giving up to \$4,000 in instant credit to anyone who
applied, even
if they shouldn't have qualified.

[http://www.nbc4.com/money/14702622/detail.html?
treets=dc&tml=dc_12pm&ts=T&tmi=dc_12pm_1_10500211272007](http://www.nbc4.com/money/14702622/detail.html?treets=dc&tml=dc_12pm&ts=T&tmi=dc_12pm_1_10500211272007)

Gabriel Goldberg, Computers and Publishing, Inc. (703)
204-0433
3401 Silver Maple Place, Falls Church, VA 22042
gabe@gabegold.com

⚡ DSL outage hits some AT&T customers (Yahoo! News)

<Stephen W Smoliar <smoliar@sbcglobal.net>>
Tue 04 Dec 2007 06:41:08 -0800

Some AT&T customers in nine states in the U.S. Southeast were
unable to
connect to the Internet via DSL for several hours on the evening
of 3 Dec
2007, officially ``because of an equipment problem'' -- although
AT&T's
domain servers were reportedly suspected. Dave Burstein (editor
of DSL
Prime) is quoted: ``Broadband goes down much more often than
telephone lines
because they didn't build the system for the same level of
reliability.''

Yahoo! News, 4 Dec 2007 <http://news.yahoo.com/> [PGN-ed]
http://news.yahoo.com/s/ap/20071204/ap_on_hi_te/at_t_outage

My own feeling is that the system vulnerability is not the
problem. Rather,

it is the casual acceptance of the vulnerability and the comparatively lame excuse for it. My guess is that we shall see more stories like this on the broadband front for both wired (e.g. cable) and wireless connectivity. Steve

⚡ Drunk a better guide than sat nav (Shapir, [RISKS-24.91](#))

<Dan Jacobson <jidanni at jidanni.org>>
Wed, 21 Nov 2007 04:48:51 +0800

> Village auto crashes blamed on sat nav

Ah! Every time somebody uses a GPS to get to my house, <http://maps.google.com/maps?q=24.181706,120.866039&t=h&z=14> they need to pay the local drunk to escort them the 13 kilometers back around the north way, as that fat juicy (to the GPS) south road just doesn't connect!

<http://maps.google.com/maps?q=24.181706,120.866039&z=15>



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



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Search RISKS using [swish-e](#)

Volume 24: Issue 93

Sunday 30 December 2007

Contents

- [Computer Failure Causes Closure of Seattle Downtown Transit Tunnel](#)
[Jason Axley](#)
- [Breakdown of aircraft separation, Sydney 4 April 2007](#)
[Andrew Rae](#)
- [Nitrogen Used To Fill Aircraft Oxygen Systems](#)
[PGN](#)
- [Army to use Macs to prevent hacking](#)
[Peter Houppermans](#)
- ['Wrong country' sat-nav blunder](#)
[Richard Weir](#)
- [Man pleads guilty to attempted shutdown of state's power grid](#)
[Paul Saffo](#)
- [FedEx Contemplating A Move to Kyrgyzstan?](#)
[Robert Mathews](#)
- [Ohio vote tampering opportunity?](#)
[Paul Saffo](#)
- [Colorado Decertifies Voting Machines](#)
[Ken Dunham](#)

- [A new low in phishing?](#)
[Andrew Koenig](#)
 - [Re: Computer Glitch Leads To Brawl At Wauwatosa Kmart](#)
[Howard Israel](#)
 - [Re: Whole of UK Child Benefit records on CD lost in the post](#)
[Tony Wright](#)
 - [Re: Private details/UK Government disks](#)
[Rob Slade](#)
 - [HMRC Lost Discs & Encryption](#)
[Brian Gladman](#)
 - [Drunk a better guide than sat nav](#)
[Jay R. Ashworth](#)
 - [Risk of poor capacity planning, etc.: online auction](#)
[Steven Hooper](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Computer Failure Causes Closure of Seattle Downtown Transit Tunnel

<Jason Axley <jason@axley.net>>
Mon, 17 Dec 2007 22:06:03 -0800

Who would have thought a tunnel would be subject to a computer failure? But alas, after the multi-year tunnel retrofit that recently completed, it seems as if all of the tunnel systems are now controlled by a single computer system that has failed. Too many eggs in one basket...

The downtown Seattle bus tunnel is closed for the night and may not be open for Tuesday's commute because of a failure of the computer system that controls tunnel operations. Transit officials are asking riders to check the metro transit Web site after 4 a.m. Tuesday morning

to see if

the tunnel will be open. The Web site is www.kingcounty.gov/metro

<<http://www.kingcounty.gov/metro>>. Riders should check timetables online

under the heading "When the tunnel is closed," which is the same routing

buses use on nights and weekends. All of the systems in the tunnel -- as

ventilation, lighting and signals -- controlled by a computer system

installed during the recent retrofit of the tunnel. Sound Transit is

responsible for that system, and is trying to fix it, a Sound Transit

spokesman said. [Source: Computer failure closes downtown bus tunnel,

Seattle Times staff]

http://seattletimes.nwsources.com/html/localnews/2004078843_webtunnelclosed17m.html

✶ Breakdown of aircraft separation, Sydney 4 April 2007

<Andrew Rae <ajrae@ssqe.com.au>>

Tue, 18 Dec 2007 10:07:26 +1000

On 4 April near Sydney, Australia, a loss-of-separation incident occurred

between a Boeing 737 and a Airbus A330. The immediate cause of the incident

was incorrect data entry by the air traffic controller. A contributing

factor was that the controller was, as per normal practice, reconfiguring

his workstation to his personal preferences at the time of the incorrect

data entry. This task normally takes over a minute, and is a distraction

from the controllers' safety critical tasks.

Other jurisdictions provide an overlap between operators to allow for such tasks.

http://www.atsb.gov.au/publications/investigation_reports/2007/AAIR/aair200701982.aspx

✈ Nitrogen Used To Fill Aircraft Oxygen Systems

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

Fri, 21 Dec 2007 21:24:51 -0600

Airlines all over the world are being warned to check to make sure there's actually oxygen in their aircraft oxygen systems after an embarrassing mix-up by Qantas Airlines at Melbourne International Airport. For ten months, crews have been filling airliner oxygen systems from a nitrogen cart that's supposed to be used to fill tires. The mistake went unnoticed until a couple of weeks ago when an observant aircraft engineer spotted service workers using the cart. "He was walking around the plane and asked what they were doing. When they said they were topping up the oxygen, he said, 'No you're not, that's a nitrogen cart,'" an unnamed source told **The Age**. As anyone who works with industrial gases knows, oxygen tanks have different fittings than other gases to prevent exactly this kind of mix-up. However, when the crews discovered the fittings on what they thought was their new

oxygen cart didn't fit, they swapped them for the ones on the old cart they were retiring. Of course, Australian officials are looking into the error and Qantas has been busy notifying other airlines that use its services in Melbourne. Hundreds of aircraft may be affected.

http://avweb.com/avwebflash/News/NitrogenUsedToFillAircraftOxygenSystems_196776-1.html

⚡ Army to use Macs to prevent hacking

<Peter Houppermans <peter@houppermans.com>>

Fri, 21 Dec 2007 22:21:05 +0100

"[...] the military is quietly working to integrate Macintosh computers into its systems to make them harder to hack. That's because fewer attacks have been designed to infiltrate Mac computers, and adding more Macs to the military's computer mix makes it tougher to destabilize a group of military computers with a single attack [...]"

http://www.forbes.com/home/technology/2007/12/20/apple-army-hackers-tech-security-cx_ag_1221army.html

<http://preview.tinyurl.com/29xelf>

⚡ 'Wrong country' sat-nav blunder

<Richard Weir <tech@vif.com>>

Sat, 22 Dec 2007 07:17:03 -0500

[Another report from the BBC regarding 'blind' faith GPS. It boggles the mind.]

Shoppers on a Christmas trip to France were taken to the wrong country after a satellite navigation blunder diverted their coach seven hours off course. Instead of arriving in Lille, France, 50 members of Cheltenham and Gloucester (C&G) Social Club were taken 98 miles (157km) away to Lille, Belgium. "Unfortunately the driver from the coach company we commissioned made a blunder on his satellite navigation."

Story from BBC NEWS, 11 Dec 2007

<http://news.bbc.co.uk/go/pr/fr/-/1/hi/england/gloucestershire/7139603.stm>

⚡ Man pleads guilty to attempted shutdown of state's power grid

<Paul Saffo <paul@saffo.com>>

Sun, 16 Dec 2007 17:28:24 -0800

[Now, why do you suppose they had the "power off" button to begin with?!? -p]

A Sacramento County computer technician has pleaded guilty to trying to shut down California's power grid by pushing a button marked "Emergency Power Off," authorities said. Lonnie Charles Denison, 33, of South Natomas, admitted Friday in U.S. District Court in Sacramento that he went into a room at the Independent System Operator's data center in Folsom (Sacramento County) on April 15, broke a glass cover and pushed the button,

prosecutors

said. Denison, a contract employee at the data center, was upset with his employer, authorities said.

The ISO oversees electricity purchases and distribution. Denison prevented the data center from communicating to the electricity market for about two hours, leaving the electrical power grid vulnerable to shortages, Matthew St. Amant, a California Highway Patrol officer assigned to an FBI task force, wrote in an affidavit. No blackout occurred because the incident - which cost \$14,000 for 20 computer specialists to repair - happened on a Sunday, investigators said. Denison was identified by surveillance-tape footage and his security-access code, the affidavit said. He pleaded guilty to attempted damage of an energy facility, a felony. He is to be sentenced Feb. 29 by U.S. District Judge Garland Burrell. [Source: Henry K. Lee, *San Francisco Chronicle*, 16 Dec 2007, C3; hlee@sfchronicle.com; PGN-ed]
<http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2007/12/16/BACHTVEM6.DTL> (Henry

🔥 FedEx Contemplating A Move to Kyrgyzstan?

<"Prof. Robert Mathews (OSIA)" <mathews@hawaii.edu>>

Fri, 28 Dec 2007 02:54:37 -0500

Could it be that FedEx is contemplating a move of their global operations from Memphis, TN, to Bishkek, Kyrgyzstan? What are the RISKS?

If FedEx were to consider Bishek as a base of operations, they would be well advised to note that SWECO's analysis did not involve components (either traffic or operational) that affect the 'bi-directional' and 'multi-directional' movement of global freight, or the possibility of the enterprise either being enhanced or enriched by the emplacement of a 'multi-point,' operation and distribution - Logistic Control System (LCS). In comparison, Santa's yearly trip as it stands, is at least thought of as being 'uni-directional' and 'load-insensitive.'

Further, as an engineering firm, SWECO does not provide any information as to what sort of improvements/savings in terms of time, efficiency, reindeer food and methane emissions*** can be expected by the proposed need to re-locate... :-). Also, the SWECO Web-site prefers that clients connect using IE 5.0 or Netscape 4.7, and not a Mozilla-Firefox browser.

Santa Claus should live in Kyrgyzstan

<http://www.sweco.se/templates/Page.asp?id=19592&print=1>

Experts at the consulting engineering company SWECO have come to the conclusion that Santa Claus should live in Kyrgyzstan. By starting his journey there, Santa can achieve the most efficient around-the-world trip to distribute Christmas gifts. He can eliminate time-consuming detours and avoid subjecting his reindeer to undue strain.

One of SWECO's areas of expertise is the use of geographic information and maps, for example to plan transports in an optimal manner. In order to

calculate Santa's ideal route, they have also studied where children live, the Earth's rotation and various demographic data to find our planet's demographic centerpoint.

Identifying Santa's optimal Christmas route is not just something we do for fun. SWECO uses the same technique when carrying out assignments on behalf of our clients. For example, we have helped numerous transport companies to optimise their routes as a means for shorting their driving distances, reducing negative impact on the environment and saving money, all at the same time!

*Why figure out where Santa Claus should live?

*This is a good exercise, and not just for fun. In recent years we have tried to think up original ideas for Christmas cards and gifts to our clients. One year we gave our clients blueprints for a gingerbread house, to highlight the fact that we have architects in the Group. This year we have chosen to show how GIS can contribute to a peaceful holiday season.

*Why Kyrgyzstan?

*A geographic and demographic analysis shows that Kyrgyzstan is located close to the richly populated countries of China and India and a ways up on the more densely populated northern hemisphere. This is also an ideal place to live if Santa Claus starts in eastern Asia and then continues his Christmas journey in a westerly direction. He would then be traveling against the Earth's rotation, which would give him twice as much time to deliver gifts

to all of the world's children.

By starting his journey there, Santa can achieve the most efficient around-the-world trip to distribute Christmas gifts. He can eliminate time-consuming detours and avoid subjecting his reindeer to undue strain."

*Santa Claus has very little time to make each stop, is it really possible?

*Yes, it is, but his extreme speed is also the reason why we rarely meet him. You might like to say hello, shake his hand and give him a pat on the shoulder, but by the time you get around to it he's already in the next town.

Where Santa Claus should live:

Latitude, (N)40.40 °

Longitude, (E) 74.24 °

*For more information:

*Rebecka Gunner, Press Officer SWECO +46 (0)734-126675, rebecka.gunner@sweco.se <mailto:rebecka.gunner@sweco.se>

[Source: Kyrgyzstan touted as ideal delivery hub for Santa, 24 Dec 2007]

<http://www.reuters.com/article/oddlyEnoughNews/idUSEIC47011920071224?feedType=nl&feedName=usoddlyenough>

*** Raymond Hainey, "Santa told to sack his gas-emitting team of reindeer,"

The Scotsman, 24 December, 2005

<http://news.scotsman.com/ViewArticle.aspx?articleid=2689094>

Ohio vote tampering opportunity?

<Paul Saffo <paul@saffo.com>>

Sun, 16 Dec 2007 17:29:59 -0800

'Tis a great day for stupid computer tricks! -p

Hanna Siegel, 16 DEC 2007, Wanna Change Votes in Ohio? Use a PDA and a Magnet;

Study Finds Ohio's Voting System Is Seriously Flawed

<http://abcnews.go.com/Politics/story?id=3D4008511>

Got a PDA and a magnet? You could switch votes cast in an Ohio election by connecting your PDA to the voting machine.

A study conducted over a two-month period this year found that Ohio's voting systems are seriously flawed. An 86-page report released by Ohio Secretary of State Jennifer Brunner says, "The findings in this study indicate that the computer-based voting systems in use in Ohio do not meet computer industry security standards, and are susceptible to breaches of security that may jeopardize the integrity of the voting process."

When Brunner was campaigning for her office seat, she promised a top-to-bottom overview of Ohio's voting system. Her findings have broad implications. With the election less than a year away, Ohio is an important swing state, decisive in returning President Bush to office in 2004.

A team of researchers from Microsolve Inc., Penn State and the University of Pennsylvania found critical security failures in all five voting systems used across the state. The software is problematic, as well. The report found that servers crashed easily. Crashes in 2007 delayed results for hours.

Brunner recommends that all touch-screen machines in Ohio be replaced with optical scan paper ballot machines, so that the results can be more easily verified. "We know this type of system will work because [many states] already use it," she said.

Brunner was not Ohio's secretary of state when the current voting machines were purchased. When asked why flawed systems were put into operation, she replied, "I'm dealing with the system that I inherited."

🔥 Colorado Decertifies Voting Machines

<"Ken Dunham" <kdunham@rogers.com>>

Wed, 19 Dec 2007 11:39:30 -0500

<http://blogs.zdnet.com/projectfailures/?p=3D541>

Coming quick on the heels of a scathing voting machine report

<http://www.sos.state.oh.us/sos/info/EVEREST/14-AcademicFinalEVERESTReport.pdf>

from the Ohio Secretary of State (see Larry Dignan for details), <<http://blogs.zdnet.com/security/?p=3D753>> the machines have been decertified for use in parts of Colorado.

According to The Denver Channel

<<http://www.thedenverchannel.com/politics/14875334/detail.html>> :

Secretary of State Mike Coffman cited security or accuracy problems in the decertified machines. A number of electronic scanners used to count ballots were also decertified, including a type used by Boulder County. Coffman

said the system had a 1 percent error rate when counting ballots. ``So for every 100 ballots we tested, we found there was an error with one of those ballots,' ' Coffman said.

The post-election random audit on which the decertification was based:

<http://www.elections.colorado.gov/DDefault.aspx?tid=3D833>

Detailed county-level audit results:

<http://www.elections.colorado.gov/DDefault.aspx?tid=3D989>

Ohio and Colorado are only the latest states to experience voting machine problems. Rest assured, there are many more voting machine screw-ups and decertifications to come. Folks, this story has hardly begun.

⚡ A new low in phishing?

<"Andrew Koenig" <ark@acm.org>>

Tue, 11 Dec 2007 17:07:29 -0500

[I got the following today--text, not HTML--purporting to be from service@paypal.com:]

Your account has been temporarily inactivated due to our general security policy. In order for us to activate your account, please send the following documents:

- 1) Send us a copy of all Credit Cards, both front and back
- 2) Send us a copy of a valid identification document (passport, driver's license)
- 3) Send us a copy of any utility bill (bank statement, electricity, insurance) with your name and address on it.

Please fax your documents to (888) xxx-xxxx.

We assure you that your personal data and documents will not be transferred to third parties.

Please note that all information which is sent by fax has to be clearly readable, otherwise we will need to re-request the verification documents.

If you should require further assistance, please contact us again as we are at your service 24 hours a day, 7 days a week.

Thank you for using PayPal
The PayPal Team

[Do people really fall for this? ARK] [Yes. PGN]

[Re: Computer Glitch Leads To Brawl At Wauwatosa Kmart \(RISKS-24.92\)](#)

<"Howard Israel" <Howard.Israel@fidessa.com>>
Tue, 27 Nov 2007 09:30:23 -0500

Interesting secondary consequences:

"One witness told police someone went to another Kmart, got some applications there and was selling them in the Wauwatosa Kmart parking lot for \$20 apiece."

Who could predict such things?

Computer Glitch Leads To Brawl At Wauwatosa Kmart; 2 People Arrested

26 Nov 2007, excerpted <http://www.wisn.com/news/14697601/detail.html>

A melee at a Kmart store in Wauwatosa Saturday morning was started by a computer glitch. The store was running a promotion in which it would give away \$10 to anyone applying for its credit card, but the computer glitch led to everyone's application being granted -- bestowing up to \$4,000 in instant credit to anyone who applied even if they shouldn't have qualified. Once word started to spread about the so-called "free money" Saturday, witnesses said things got pretty nuts inside the Wauwatosa store. "They were having a big fight. Two ladies was jumping a lady over credit cards," witness Sylvester Wilson said.

Nearly a dozen Wauwatosa squad cars responded to the call just before 11 a.m. Saturday for what was called a large fight in progress. "It was a nice brawl. It came from inside to outside. If you go up there, you'll see hair, earrings, all pulled out on the ground," Wilson said.

What started as a fight between two women in the crowded store evolved when several men intervened. A store employee got punched in the nose and crashed through a glass display case. He was treated for a broken nose and various cuts. Two suspects, a 22-year-old man and a 16-year-old boy, were arrested, accused of battery.

Meantime, Kmart is still trying to clear up the credit card mess.

Two employees confirmed for police that anyone who applied was being given

instant credit -- from \$850 up to \$4,000. They also told police that people started calling other people to the store for so-called free money. The store ran out of credit applications. One witness told police someone went to another Kmart, got some applications there and was selling them in the Wauwatosa Kmart parking lot for \$20 apiece. Kmart would not comment on how many people got the credit cards who shouldn't have or how much merchandise they were able to buy with them.

Previous Story: November 24, 2007: Brawl Breaks Out At Kmart
<<http://www.wisn.com/news/14682561/detail.html>>

Howard Israel, Corporate Security Officer, Fidessa Corporation
Howard.Israel@fidessa.com <mailto:Howard.Israel@fidessa.com>
(212) 320-3315

Re: Whole of UK Child Benefit records on CD lost in the post

<Tony Wright <adw@saska.co.uk>>
Tue, 18 Dec 2007 23:12:22 +0000

(Mellor, [RISKS-24.92](#))

The danger here is in misunderstanding what service you are buying. In Royal Mail (I've no idea what the 'In house' TNT service does) what actually happens is this:

Recorded Delivery means that the package or letter goes totally untraced with regular mail until such time as it is Delivered or returned by the postman to the sorting office as Undelivered. If it is delivered

it should
be signed for by the recipient -- upon return to office the
postman hands in
the delivery sheet and the item is only then entered into the
system as
Delivered. If undelivered, then a notice should be left and the
item is only
then logged into the system when the item is returned to the
office. AKA
Nothing is traced until a delivery is attempted. If the item
doesn't shake
out of the bottom of a bag in a sorting office somewhere, there
is no more
way to trace where it is during its journey than any piece of
regular mail.

Special Delivery, AKA what was referred to as Registered Mail
(which no
longer exists) is signed for, barcode traced and receives
special handling
throughout its entire journey from when it is posted at a Post
Office to
when it is delivered.

The thing about Recorded Delivery is that if uncollected it must
be returned
to sender after 7 days and is therefore used as a legal
instrument of
notification in the UK.

✉ Re: Private details/UK Government disks (Houppermans, [RISKS-24.92](#))

<Rob Slade <rMslade@shaw.ca>>
Mon, 17 Dec 2007 20:38:05 -0800

"The department had a detailed manual covering procedures for
handling the

benefits database and other sensitive information. However, the manual itself was considered too sensitive to be widely distributed, so it was restricted to civil servants only, The Guardian reports." http://www.theregister.co.uk/2007/12/17/hmrc_manual/.

("Civil servants" are senior staff.)

rslade@vcn.bc.ca slade@victoria.tc.ca
rslade@computercrime.org
<http://victoria.tc.ca/techrev/rms.htm>

✶ HMRC Lost Discs & Encryption

<Brian Gladman <brg@gladman.plus.com>>
Tue, 18 Dec 2007 09:26:38 +0000

The discs lost by HM Revenue & Customs were password protected with WinZip version 8, which means that encryption was used but it was relatively weak and subject to both password search and known plaintext attacks. It is very unlikely to hold up against a determined attacker.

WinZip version 9 introduced an AES based approach with a conservative design that had good protection against password searches and known plaintext attacks. With a good non-dictionary password I believe this would hold up against even the most determined attack had this been used in the HMRC scenario.

⚡ **Drunk a better guide than sat nav (Jacobson, [RISKS-24.92](#))**

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

Tue, 18 Dec 2007 10:56:07 -0500

It's a little troubling to me that none of the articles that seem very popular lately on "how dangerous it can be to depend entirely on your satellite navigator" make clear the point -- obvious to technical people, but not always to civilians -- that the problem is *actually* failures in the *mapping and routing data*, and nothing directly to do with the satellites themselves.

The RISK? Well, it's a slightly obscure one; the opposite of what we usually deal with around here: it's a bad idea to *reduce* the confidence of the general public in something which really *is* pretty stable; GPS in itself is pretty accurate and doesn't break much.

In case you've never noticed, almost no one ever says "run on a bank", even when that's what's actually happening. Same reason. Mass psychology.

Doesn't pay to ignore it.

Jay R. Ashworth, Ashworth & Associates, St Petersburg FL USA +1 727 647 1274
<http://photo.imageinc.us> <http://baylink.pitas.com> jra@baylink.com

⚡ **Risk of poor capacity planning, etc.: online auction**

<"Steven Hooper" <shoobe01@gmail.com>>

Fri, 21 Dec 2007 16:50:18 -0600

The .mobi TLD is a relatively new one, specifically to address websites for mobile browsers. The organization that runs it, promotes it and sort of makes money helping get folks' sites working has periodic auctions of some of the more in-demand names. The latest group of these ended 5 December, 2007

As detailed here:

<http://dotmobi.typepad.com/dotmobi/2007/12/open-letter-to.html>

There were some problems with it. Quoting the salient part:

> We have noticed that some people seem to believe that the auction participants who received notifications and invoices before the extension of the auction were the highest bidders at the close of the original auction period.

>

> Sedo, however, tells us that:

>

> a) this is clearly not true in some cases,

> b) this is unlikely to be true for the names generating the most activity,

> and

> c) this is possibly not true for any of the auctions.

>

> To those points, Sedo has told us the following:

>

> - As the scheduled auction end approached, bidding activity increased dramatically, creating significantly higher-than-expected traffic.

> - Although the web interface slowed down for some participants, the auction interface and bid page remained available for many or all users, and

> the web servers continued to log incoming bids.
> - Once the bid processing server stopped functioning properly,
> however, many of those bids -- both standard and proxy -- did
not get posted
> to the bid history page.
> - As a result of the server crash, another system automatically
> generated email notices at 5 p.m. GMT to the highest bidder
listed
> on the bid history page, despite Sedo's attempts to stop that
process.
> - Because the bid history page did not reflect all of the valid
> bids, notices were sent to some participants who were not, in
fact, the
> highest bidders.

Some interesting information is revealed. Aside from the failure
of Sedo
(or, it seems /anyone/) to accurately predict and provide for
capacity, is
the poor capacity planning. In the broader sense, there should
have been a
provision for failure of this sort.

My core issue here is of this phrase, "...another system
automatically
generated email notices at 5 p.m. GMT to the highest bidder
listed on the
bid history page..." This strikes me as particularly poor
planning. Sending
notices should probably not simply be at a time, but upon a
sending of "win"
status. That alone would have

Even worse is the end of the same sentence, "...despite Sedo's
attempts to
stop that process." If true (and not simply spin in the
aftermath), having
no good way to stop cronjobs, or sending of data seems like a
serious
failure on the part of a system with a notable public presence,
and an often
non-trivial financial commitment on the part of the end users.

Entirely aside from designing the system to post, check, and confirm data, simply planning for component outages should have revealed this failure.

Capacity testing, likewise, should have been performed to failure on individual components, and likewise should have revealed this failure condition.

Note that although I work in the mobile industry, I did not have a bid in on any of these domains, winning or otherwise, so have no specific stake in the outcome of this event.



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